Solution Guide

BSG8ew 1.0

Small and Medium Business

Document Status: **Standard**

Document Number: **NN47928-200**

Document Version: **01.01**

Date: **March 2008**

NORTEL

Copyright © 2008 Nortel Networks, All Rights Reserved

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Introduction **7**

Solution overview **9**

Scope of solution and this document 9
Solution description 9
Configuration and deployment of release 1 / SMB data portfolio 12
Network management 14
Quality of Service 17
Data services 20
Voice services 20
Security 22
Wireless LAN capabilities 24
Monitoring and reporting 25

Solution components **27**

BSG8ew 27
LG-Nortel LIP- 6800 series IP phones 28
Key features 29
LG 6000 series SIP phone key attributes 30
MCS PC client 31
IPSec VPN client 31
BES 31
BAP 120 32

General considerations **33**

Deployment strategy 34
Pre-configuration requirements 34
BSG8ew interfaces 36
WAN interface 36
LAN interfaces 37
LAN to WAN routing 38
IP address allocation 39
SSID to VLAN mapping 39
End-to-end Quality of Service 39
Service based QoS requirements/DSCP marking 43
BSG8ew default DSCP to 802.1p mapping 44
Egress queue setting 45
VLAN to WAN or VLAN to VLAN QoS implementation 45
IP phones connected directly to the BSG8ew LAN port 48
IP phones connected to the L2 switch 49

IP Phone and PC share the same L2 switch port 51
QoS implementation for PC soft phone 51
Security 52
Secure management access 52
NAT, Firewall, and ALG 53
Authentication 54
Customer network partitioned into VLANs 57
Service availability 57
Call routing to the PSTN network 57
BSG8ew backup mode in case of WAN interface failure 58
Network management 58
Software Upgrades and Backup and Restore 60
BSG8ew 60
LG 6000 61
Business Ethernet Switch 61
Voice calls 61
SIP proxy and registrar 61
SIP ALG 62
Call Admission Control 62
Call server failover 63
Analog telephony and FAX 63
Emergency voice calls 64
Dial plan 64
Data services 65
Host network considerations 65
WAN QoS strategy 65
Interoperability requirements and summary 67
Voice services 67
Data services 67
Performance and capacity summary 67
Reference topologies 69
Topology 1 — Data and SIP voice services 70
Configuration steps 71
Topology 2 - Data and SIP Voice with port expansion and mobility 80
Configuration steps 81
BES50 configuration 81
BAP120 configuration 85
Topology 3 - Data and SIP voice with IP VPN between main and branch site 88
Topology 4 - Data and SIP voice with IPSec client termination (teleworking) 92
Solution components configuration example 95
Overview and objective 95

Operational assumptions 95
Single site topology 95
Operating mode 96
Required services 97
Post installation configuration of BSG8ew 100
Pre-deployment configuration of BES50 116
Pre-deployment configuration of BAP120-A 127
Pre-deployment configuration of LG6800 series phones 146
Pre-deployment configuration of SafeNet VPN client 151
Site to Site VPN topology 160
IPSec main site configuration 160
IPSec branch site configuration 161
Appendix A – SMB solution integration with BCM50 163
Single site — UNISTIM phones only 163
Single site — UNISTIM and LG phones 165
Site-to-Site configuration 166
Appendix B – QoS architecture of BSG8ew 169
Classification 169
Congestion control 170
Meter / Policer 170
Scheduler 173
Call admission control 173
Appendix C - BSG8ew services 175

Introduction

The Solution Guide describes the integration of Business Services Gateway (BSG) with the SMB portfolio and the CS2K for Nortel Hosted Solutions. This guide is intended as a reference guide for BSG for application programmers, engineers, and system administrators. Ensure that you have *BSG 8ew Administration Guide* (NN47928-600) and *BSG 8ew Configuration Guide* (NN47928-500) with you.

This guide includes an overview of the following:

- Solution overview (page 9)
- Solution components (page 27)
- General considerations (page 33)
- Interoperability requirements and summary (page 67)
- Reference topologies (page 69)
- Solution components configuration example (page 95)
- Appendix A – SMB solution integration with BCM50 (page 163)
- Appendix B – QoS architecture of BSG8ew (page 169)
- Appendix C - BSG8ew services (page 175)

Derivatives of this document are intended to benefit channels that serve the converged (voice and data) communications needs of small and medium sized business. The intent of having a reference framework (that is updated and augmented over time) is to provide valuable guidelines from which channels can tailor their solutions to specific customers needs. Consideration of converged solutions is an integral part of the product design cycle. From inception, individual products are considered to be components of a solution reference design. Portfolio releases are a means of coordinating product design and delivery. This approach serves the dual purpose of lowering a reseller engineering and support costs and maximizing the value of products as components of innovative solutions.

Variations of this document will be published to capture details associated with other channels' operating environments.

Each product in SMB Portfolio shall stand alone as a competitive point solution in a mixed vendor environment, and shall be validated as a component of a high value solution reference design.

The following table lists the solution components with corresponding software loads.

- BSG8ew
- BES50 family of switches,
- Business Access Point (BAP)120
- LG 6800 Series IP phones
- Safenet VPN client
- Nortel Eybeam client SMC 3456
- Nortel MCS PC client

Table 1 - Solution components software loads

Solution component	Software load
CS2000 SSL	SN09
BSG8ew	Release 1.0
BES50 GE/FE	GE: V1.0.5.0, FE: V1.0.3.0
BAP 120	Release 1.0 [V4.3.3.7]
LG 6800	1.2.41sc
Safenet VPN client	10.8.0
Nortel Eybeam client SMC 3456	Release 1.0, Build 45629
Nortel MCS PC client	Release 4.1 [V4.1.661]

Solution overview

Scope of solution and this document

This document describes the requirements and configurations for the BSG8ew based hosted solution. The focus is on the LAN components and the WAN interface. A separate document, developed by the Network Business Solutions Group (part of Nortel Global Services) describes the Hosted Solution Center (HSC) and regional network considerations.

Solution description

The SMB Business Services Gateway (BSG) solution is designed to cost effectively deliver the rich set of multimedia services to small and medium business with reliability and security. To achieve these objectives, the solution integrates:

- A Hosted Solution architecture with centralized communication servers for multimedia service delivery.
- A compact access gateway (BSG8ew) that itself integrates several SMB services into one box: A router for layer 3 processing, SIP Registrar, Proxy, and Application Layer Gateway, an Ethernet switch for interconnecting SMB devices and a Wireless Access Point (WAP) for the wireless LAN connectivity.
- A rich set of SMB devices (The solution components are presented in the chapter General considerations (page 33)).

The following SMB products are integrated into the solution to provide data and multimedia services:

- BSG8ew
- BES50
- Business Access Point (BAP)120
- LG 6800 IP phones
- Safenet VPN client
- Nortel Abeam client SMC 3456
- Nortel MCS PC client

The BSG8ew is the central point of the SMB side of the solution, along with other solution components enables port expansion.

To satisfy complex port expansion requirements the Business Services Gateway (BSG) provides for L2 network partitioning by means of VLANs. The customer network can be expanded using Nortel BES Ethernet switches and use of the BSG8ew VLAN trunks (802.1Q) capabilities.

The BSG8ew has one designated Ethernet WAN interface and additional physical WAN interfaces are configurable.

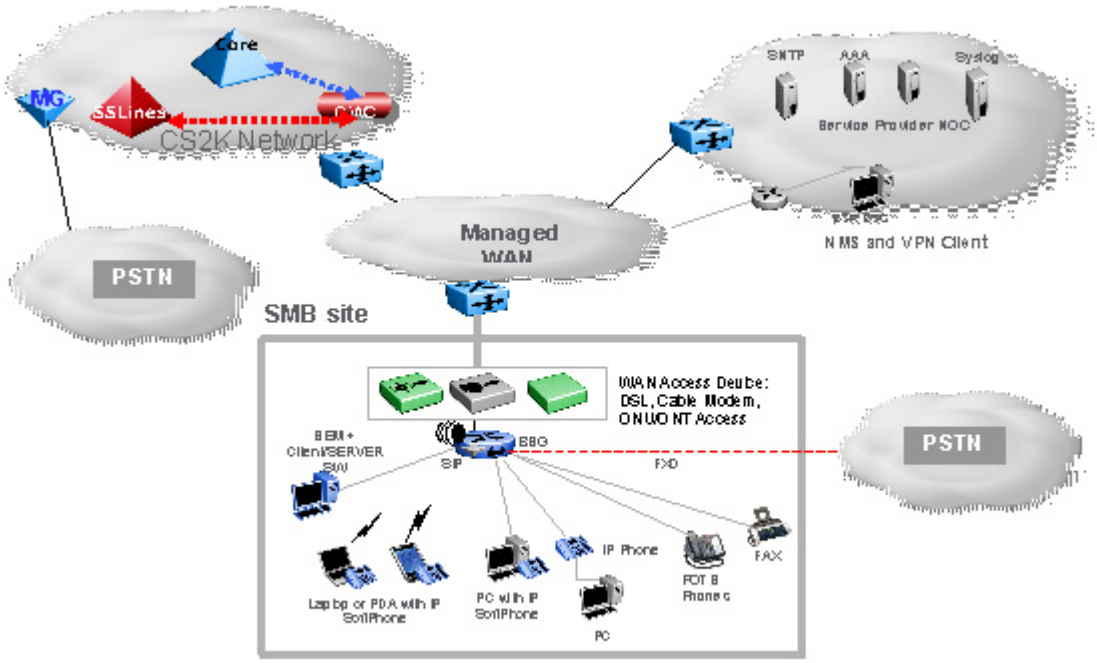
Several options are considered when connecting BSG8ew to the core network. High level view of connectivity options is presented in Figure 1 WAN connectivity options (page 10). Possible options are:

- DSL modem
- Cable modem
- ONU/ONT access

In any of the cases, BSG8ew connects to the Ethernet port of access device and the Ethernet frames are bridged towards the core network device that aggregates traffic from access links. For example, a DSLAM in case when the DSL is used for WAN connectivity.

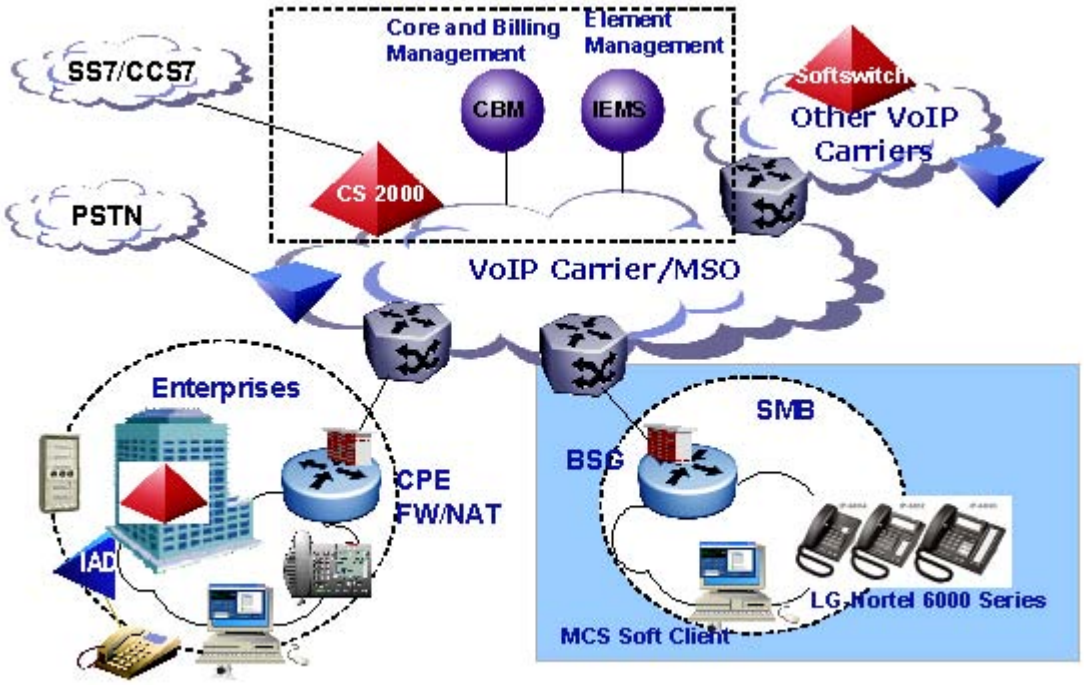
For the purpose of illustrating the solution, DSL based connectivity is used in this document, however any of the above access technologies can be used.

Figure 1 WAN connectivity options



In the hosted solution architecture, the multimedia services are hosted on the communication servers. The communication servers are the control centers that facilitate delivery of the services to the end user. Typical network architecture for hosted services is presented in Figure 2 The Hosted solution architecture (page 11).

Figure 2 The Hosted solution architecture



The shaded region indicates the solution area of focus for this document. The dashed line enclosed region (top center) represents the solution area that is addressed in respective Nortel Global Services documents. The Hosted Solution Network architecture is built around the managed IP network and involve several components. The components involved in the architecture are the Communication Servers (CS2000), Media Gateways, Signaling Gateways, and CPE devices. They are interconnected through the Managed IP network that can be viewed as a core network that is managed by the service Provider. The core network interconnects the customers as well as allowing the customers to access communication servers like CS2000. With respect to the service provider customers the core network can be viewed as a public network. In reality it is not a public network since access to it from the Internet is controlled and limited.

The hosted solution can be managed by the service provider itself. In case of Nortel hosted solution, the services are hosted by Nortel Hosted Solution Center and the service provider provides connectivity between the customer network and Hosted Solution Center through its core network.

There are certain requirements that have to be met to deliver the multimedia services, especially voice and video across the IP network. The access devices deployed in SMB enterprise site have to support these requirements in addition to standard data services. That creates a need for the specialized data devices that not only can handle packet forwarding but in addition have to facilitate seamless delivery of the services like voice and video.

Nortel BSG is such a device and it is designed to deliver managed voice and data services to small and medium enterprise customers. It is designed for reliability, scalability and capacity and at the same time for lowest cost deployment and operation, a vital consideration for carriers.

The BSG access device that allows delivery of voice and data services to the SMB. The BSG8ew is fully integrated with the SMB portfolio of devices that comprise the end customers network. In the solution, BSG8ew is managed by the service provider, off loading the end customer from the burden of managing and support of the access device. In the data domain BSG8ew has the role of access router and it supports all the services that are appropriate for this role.

The objective of this document is to provide the comprehensive description of the BSG8ew centric solution for managed voice and data services in the context of the CS2000 multimedia network architecture. It can however be expended to accommodate other multimedia service architectures. For example, by replacing CS2000 call server with another call server like Sylantro, Broadsoft.

The document helps customers to satisfy the requirements when implementing the solution into the customer network infrastructure. It is hoped that this document will lower the cost and complexity of implementing a managed service solution using BSG8ew on the customer network.

Configuration and deployment of release 1 / SMB data portfolio

To limit the configuration work required during the installation process the solution components other than BSG8ew are pre configured with the required parameters. The BSG8ew needs to be pre-configured to allow remote access to the device before shipping it to the destination location. All the solution components can be managed through the WEB browser. The BSG8ew also has very extensive CLI available for configuration and management. The typical HTTP/HTTPS management sessions are shown in Figure 3 Management connectivity (page 13).

The BSG8ew acts as a DHCP server and assign IP addresses and other parameters to the SMB devices that are required for IP based services. The BSG8ew is also ready to provide SIP proxy services to customer SIP endpoints.

There are two aspects of service provisioning that have to be taken into account when installing the solution components. One is with respect to data services that provide for secure and reliable communication for solution components. The second one is with respect to voice applications that the solution delivers and that require data services for correct operation.

The data services require configuration of:

- VLAN interfaces
- Interface IP addresses
- Default gateways
- NAT
- Firewall
- IP VPN
- QoS

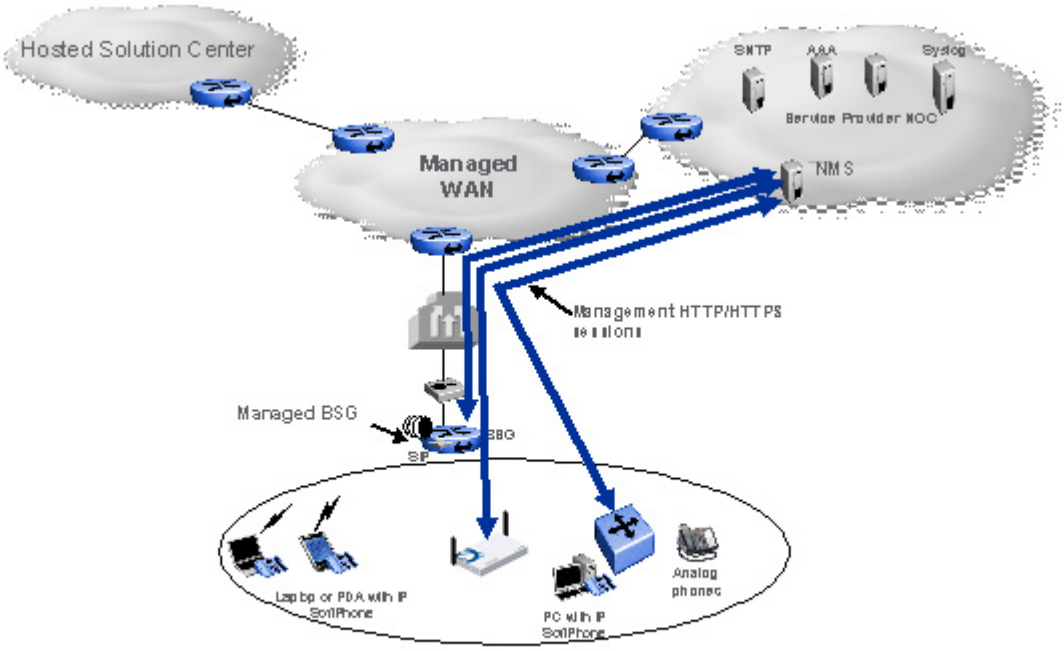
The voice services require configuration of:

- IP address of the communication server (only one communication server can be provisioned on BSG8ew)
- Home domain
- Dialing plans (normal and backup, see BAP 120 (page 32))
- Default polling value (to check if the call server is available)
- The VoIP endpoints need to be pre-configured with the IP address of the BSG8ew SIP proxy, DNS Server IP address, and the TFTP configuration server. They also need to be configured with the Home Domain and user ID and password that correspond to the user account provisioned on CS2000 SIP Server. All this information can also be distributed to the VoIP endpoints by means of the DHCP options.

Attention: The IP address of the SIP proxy and DNS server proxy is always the IP address of the VLAN 1 virtual interface. By default it is 192.168.1.1. Even if the device is not a member of VLAN 1 it needs to use IP address of VLAN 1 virtual interface, in this case 192.168.1.1, as a destination address for BSG8ew SIP and DNS proxies.

The detailed description of components configuration is provided in the chapter Solution components configuration example (page 95).

Figure 3 Management connectivity



Attention: The BSG8ew supports Authentication and Authorization but it does not support Accounting functionality.

Network management

In the BSG8ew solution, the network management of the customer network devices is handled remotely from the service provider NOC. There are several network elements located at the customer site that have to be managed:

- Business Services Gateway (BSG)
- Business Ethernet Switch (BES)
- BAP 120 Wireless Access Point(s)
- LG IP phones

Other devices that are part of the SMB customer network communicate with the NOC through the BSG8ew. This topology is presented in the remote network management application at the NOC site can securely communicate with the SMB devices by means of IPSec client tunnel that terminates on the BSG8ew. This is presented in Figure 5 IPSec client tunnel for remote management (page 16). After the VPN tunnel is established, the service provider can manage on site network elements using Business Element Manager (BEM) to discover nodes, and use obscure protocols such as HTTP. In a typical network management architecture envisaged for the solution the network management applications that include AAA (Radius or TACACS), SNTP, SysLog and NMS applications are located at Service Provider NOC site as depicted in Figure 4 Network management architecture (page 15).

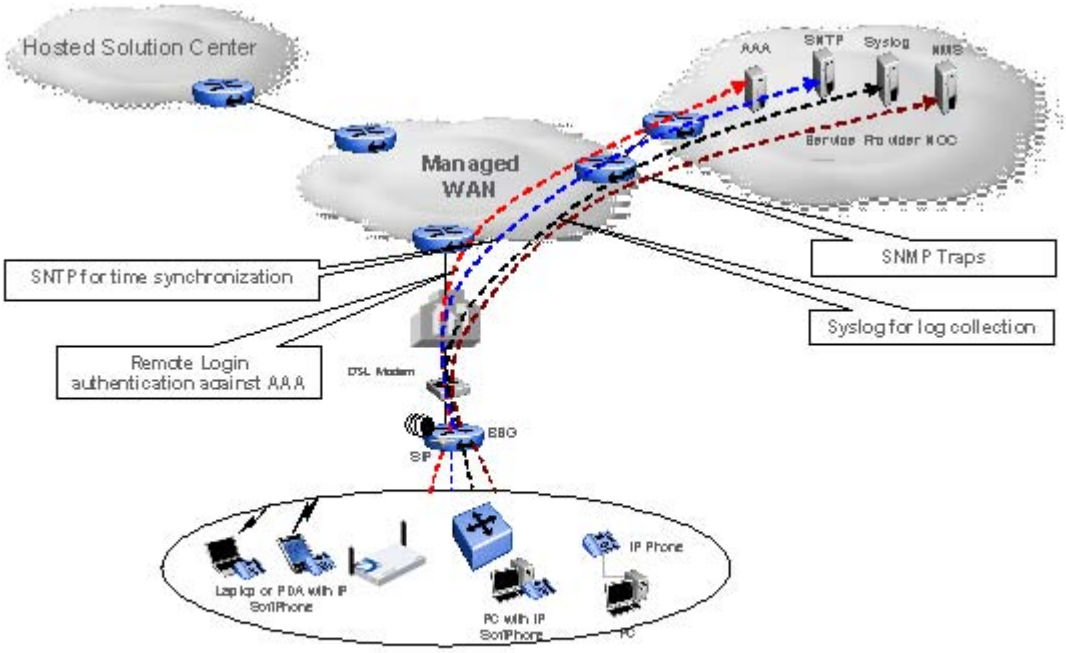
Attention: SG8ew does not have Real Time Clock thus it needs to have access to SNTP server to synchronize the time.

The in-band network management can be delivered through the use of both secure and un-secure communication between the network management components located at the service provider NOC and the BSG. BSG8ew supports several secure protocols that can be used to transport network management traffic.

Remote management of the BSG8ew is supported through secure management protocol SNMPv3. BSG8ew, HTTPS, and SSH to provide secure connectivity for management applications that can utilize these protocols for transport. BEM is such an application that uses https to securely communicate with the network element and both can be used to manage BSG8ew. Use of unsecured protocols such as HTTP, Telnet, and SNMPv1/v2c to manage BSG8ew remotely is not recommended, especially if the management traffic traverses an un-trusted domain.

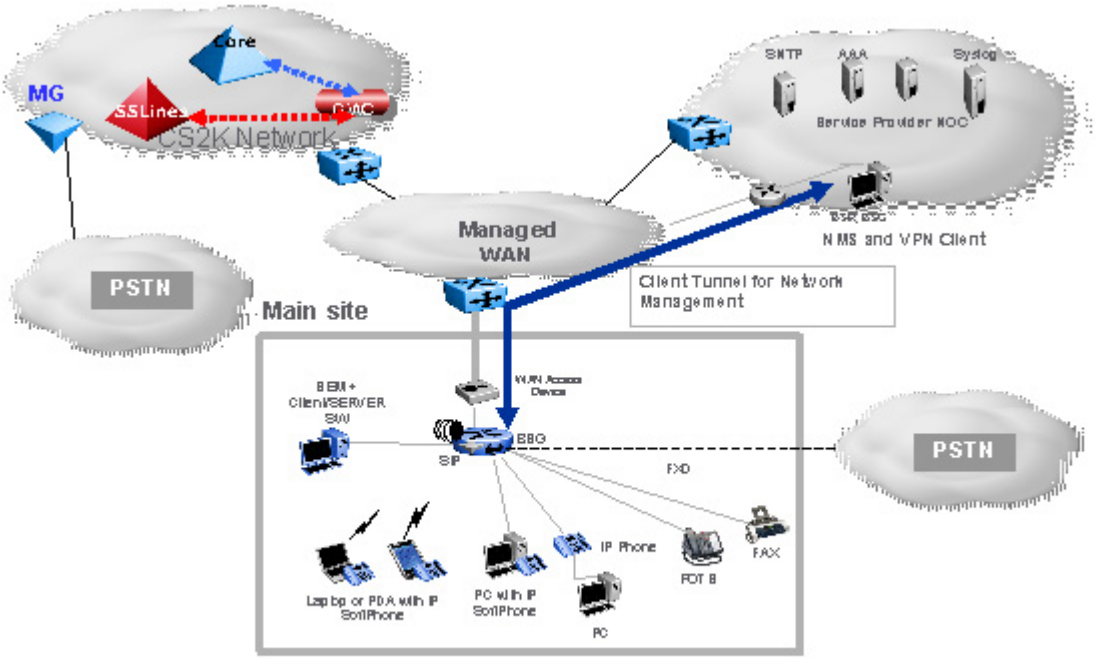
BSG8ew supports access control to control access to BSG8ew subsystems. Read-Only/ Read-Write rights are assigned to the user groups. Management views can be set on a per user account basis.

Figure 4 Network management architecture



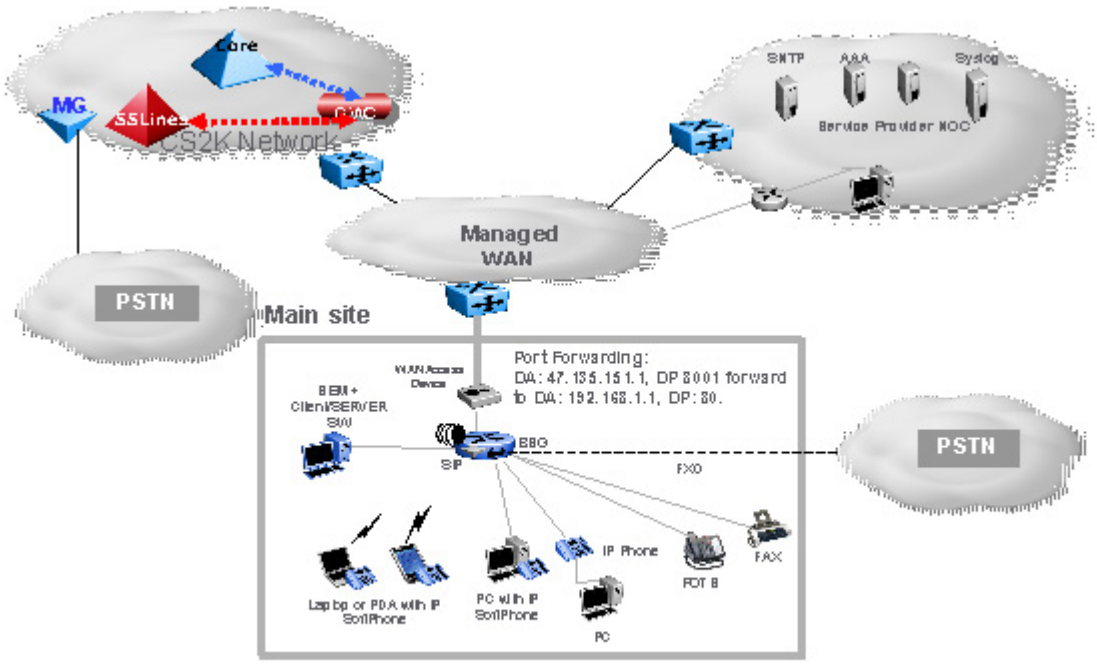
The remote network management applications at the NOC site can securely communicate with the SMB devices by means of IPSec client tunnel that terminates on the BSG8ew. This is presented in Figure 5 IPSec client tunnel for remote management (page 16). After the VPN tunnel is established, the service provider can manage on site network elements using BEM to discover nodes, and use unsecured protocols such as HTTP.

Figure 5 IPSec client tunnel for remote management



Alternatively, Figure 6 Port forwarding for remote management access (page 17) port forwarding capabilities built into BSG8ew are used to remotely manage SMB devices. The http management connection requests are forwarded to the destination device based on the destination port number in the incoming packet. Detailed description of this configuration is provided in section Network management (page 58).

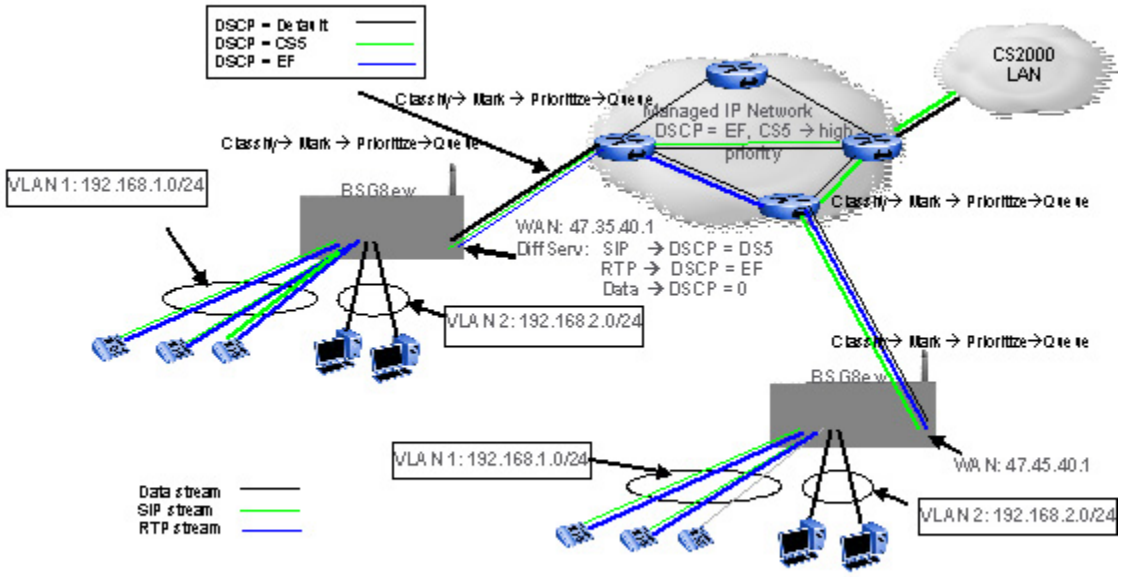
Figure 6 Port forwarding for remote management access



Quality of Service

In the SMB BSG8ew solution the BSG8ew aggregates the traffic from the devices connected to BSG8ew ports and routes it between the devices or out to the service provider network. VoIP is one of the services that the SMB BSG8ew solution delivers to the customer thus the portion of that traffic carries voice signaling and voice media bearer data. The VoIP traffic is a time-critical traffic and is very sensitive to packet loss, latency, and jitter. To limit these traffic impairments the QoS mechanisms need to be applied to the packets along the path they travel. Figure 7 Simplified view of the solution topology with End-to-end QoS presents three types of flows that can represent the type of traffic typical for SMB enterprise. The topology presented in Figure 7 Simplified view of the solution topology with End-to-end QoS (page 18) is a simplified view of the solution topology and is used here only for the purpose of presenting Quality of Service concept.

Figure 7 Simplified view of the solution topology with End-to-end QoS



The QoS needs to be applied on both LAN and WAN interfaces (Figure 7 Simplified view of the solution topology with End-to-end QoS (page 18)). For example, packets that are received on the LAN interface and are to be forwarded out the WAN interface would be classified and prioritized accordingly but also the packets that are received on the WAN interface and to be forwarded out the LAN interface would also be classified and prioritize.

To provide end-to-end QoS particularly for voice traffic, the service provider managed WAN is assumed to be diffServ environment and the BSG8ew sits at the boundary between the customer network and the service provider diffServ environment. The Egress traffic from the customer premises will be shaped and marked with DiffServ Code Point (DSCP) value according to the Service Level Agreement (SLA) between the customer and the service provider by the BSG8ew. The BSG8ew can also prioritize ingress IP packets based on the DSCP code in the IP header.The BSG8ew QoS capabilities are summarized in the following table.

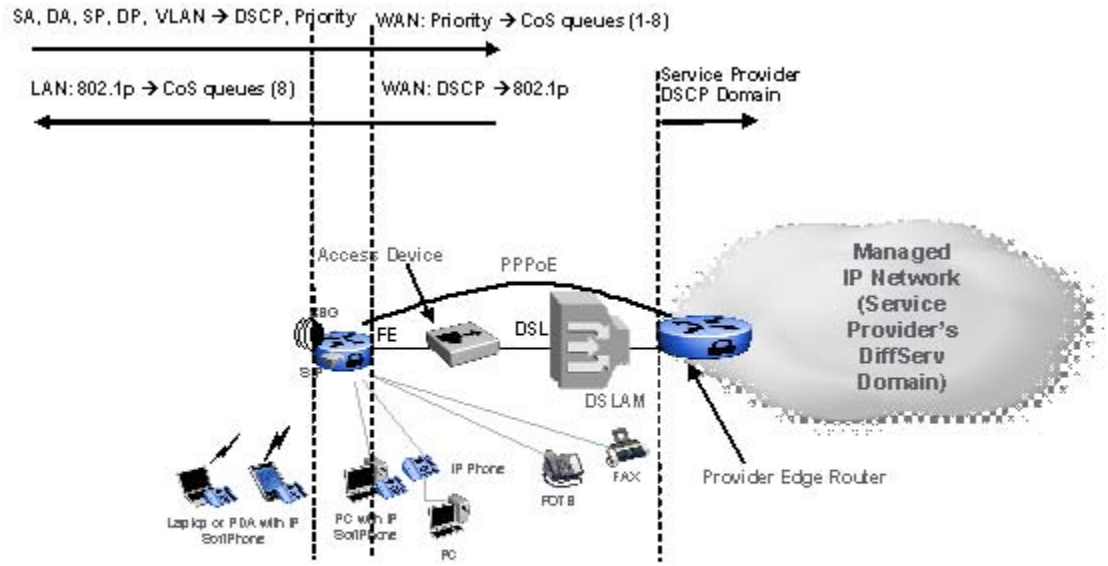
Table2 - BSG8ew QoS capabilities

QOS service	Description
Classification	The BSG8ew can classify packets based on the following fields: SA/DA, SP/DP, Protocol (TCP, UDP), DSCP, and VLAN Id/Interface.
Bandwidth Management	Two rate three color marker policer.
Queuing and Scheduling	8 priority queues (0-7); strict priority and WRR scheduling.
Congestion Control	RED, WRED for TCP flows; tail dropping for non-TCP flows.

The general high level view of QoS implementation is presented in Figure 8 Packet classification and prioritization (page 19) and its components are described in more details in subsequent sections. The details of QoS architecture are described in Appendix A – SMB solution integration with BCM50 (page 163).

These QoS mechanisms are applied correctly to ensure that the expected quality of service is achieved. The subsequent sections provide detailed description of QoS implementation for various deployment scenarios.

Figure 8 Packet classification and prioritization



The BSG8ew supports 8 degrees priority queues per port that can be used for prioritization of the traffic. There is a default DSCP to egress queue mapping available on BSG8ew for LAN to WAN direction.

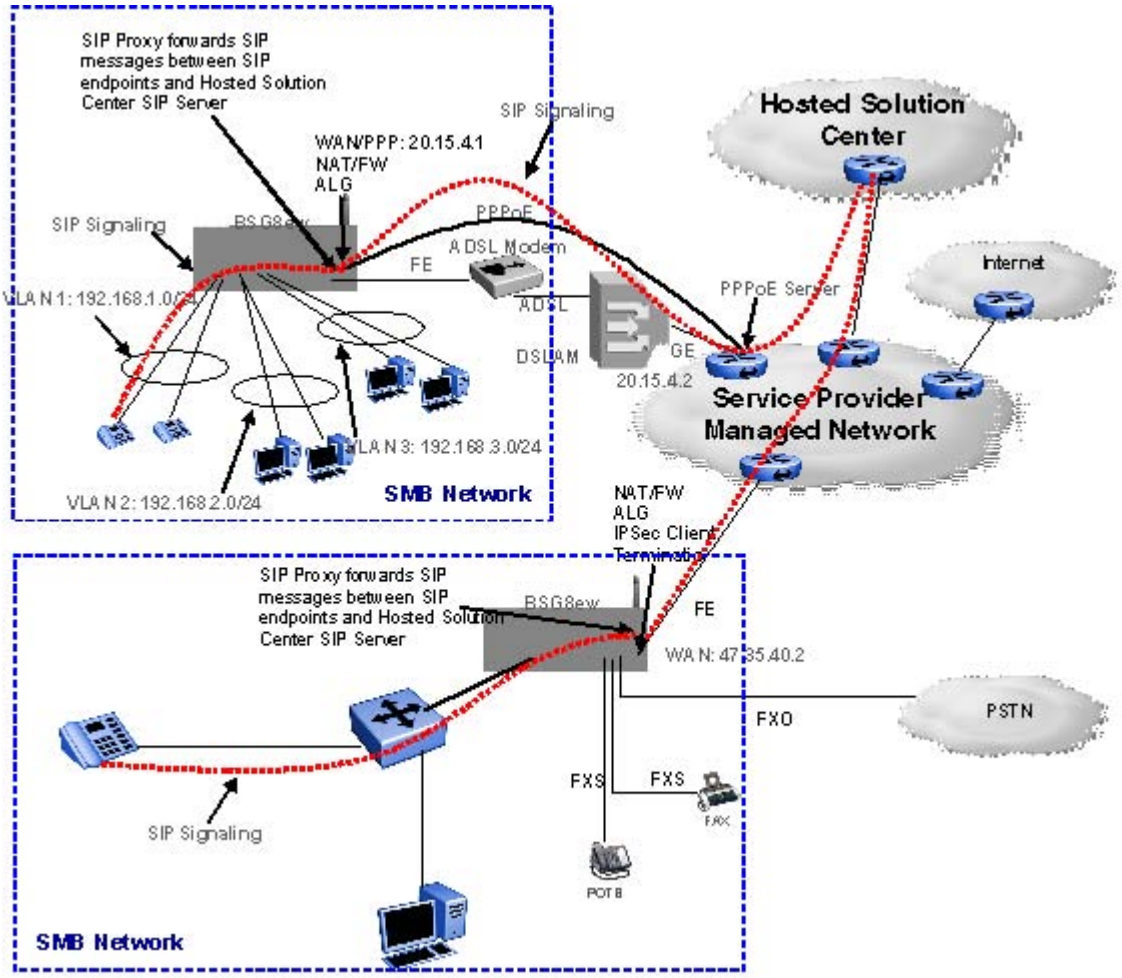
Data services

The BSG8ew solution provides for reliable and secure communication between the customer devices and the hosted solution center. In this context, BSG8ew is an access router that facilitates this connectivity. The BSG8ew supports full range of services that typical access router does support. Some of the services that are relevant to the solution are explained in subsequent sections. The detailed list of data services available on the BSG8ew is presented in Appendix C - BSG8ew services (page 175).

Voice services

The Business Services Gateway (BSG) integrated with Nortel Hosted Solution enables rich set of the SIP based voice services. In a normal mode of operation the voice services are located on the Communication Servers at the Hosted Services Center site and the BSG8ew simply proxies the SIP control messages to the Communication Servers. The BSG8ew implements enhanced SIP Proxy capabilities to facilitate SIP voice/multimedia call control between the customer devices and the SIP communication servers (see Figure 9 Hosted services control path (page 21) for details on the control path for voice calls). With the enhanced proxy capability the BSG ensures seamless communication of the customer devices with the communication servers as well as the setup of the required media path.

Figure 9 Hosted services control path



The BSG8ew supports call survivability by means of normal and backup dial plans. The BSG switches to backup mode when communication with the central SIP server is lost. The BSG8ew uses SIP options messages to monitor availability of the central SIP server. Once it is detected that the central SIP server is not available or the WAN connectivity is lost, the BSG8ew transitions to backup mode and acts as a SIP server (Proxy and SIP registrar) for the local endpoints. In a backup mode BSG routes local calls between the endpoints within the LAN. These endpoints include analog phones connected to two FXS interfaces. It can route external calls to the PSTN through the FXO interface. While in a backup mode, BSG8ew continues to monitor availability of the central SIP server, and once the server becomes available transitions to the normal mode.

The BSG8ew FXO interface provides for failover mechanism that allows emergency call to be routed to the PSTN network in case the SIP Call Server is unreachable. Since there is only one FXO interface, only one call at a time can be placed. The emergency call takes priority over non emergency call. If an emergency call is being placed over FXO interface and there is already non emergency call present, the non emergency call is terminated.

The example voice and multimedia services that are available through the Nortel Hosted Solution Architecture are presented in.

SIP lines telephony service	**SIP multimedia service**
Calling ID/Name/ Party	Address Book
Calling ID Suppressions	Chat
Decline	Make Call
Call Forward Variants (CFU, CFB, CFDA etc.)	Instant Messaging
Do Not Disturb	Click To Dial
Last Number Re dial	Click To Dial (from Microsoft Outlook)
Anonymous Caller Rejection	Clipboard Push
Call Back To Busy Line	Converged Desktop
Ad-hoc Conference	File Transfer

Security

The BSG solution uses a full range of standard security mechanisms to ensure the protection of customer network devices and to enable their secure access to both voice and data services as well as secure communication with other devices on the network.

The BSG8ew implements both a stateless and a Stateful firewall. The stateless firewall can inspect and filter packets based on the following fields:

- Protocol field in Ethernet header
- Source IP address
- Destination IP address
- Protocol
- Source port
- Destination port

The Stateful packet inspection and filtering can be performed using the following fields:

- Protocol

- Source IP address
- Destination IP address
- Protocol
- Source port
- Destination port
- TCP flags and connection state

An Intrusion Detection and Prevention capability will detect, prevent and log common Denial of Service (DoS) attacks once the firewall is enabled. The firewall can be enabled on any interface including virtual interfaces. The supported security features are listed in the following table.

Table 4 - BSG8ew security services

Service	Description
NAT	PAT, many-to-one, one-to-many, static, dynamic, reverse NAT
Firewall	Stateless (Access Control List) and stateful firewall
IDS/IPS	Supports 26 common attacks.
Port based network access control – 802.1x	
IPSec Client Termination	Supports SafeNet IPSec client; Split tunneling is not supported.
IPSec Branch Office Tunnel	Supports NAT Traversal; QoS is not available for packets entering IPSec tunnel.
Authentication	Local database, Radius, TACACS
Secure Management Access	SNMP V3, https, SSH
WLAN	Open, WEP, WPA, WPA-2, WPA-PSK, WPA2-PSK

To secure data traffic between multiple sites of an SMB, the BSG8ew supports site-to-site IPSec Branch to Branch Tunnels. Release 1.0 of the BSG8ew only supports symmetrical BOTs meaning that both the initiator and responder must be configured with the remote peer IP address.

Services and applications at headquarters can be securely made available to tele-workers and road warriors using IPSec client VPN tunnels. Remote Safenet clients are dynamically assigned IP addresses during IKE config mode. The summary of IPSec supported features is presented in the following table.

Table 5 – BSG8ew IPSec features

Feature	Description
Encryption	DES, 3DES, AES
Hash Algorithms	HMAC-MD5, HMAC-SHA1, DES MAC
Diffie Hellman Group Support	Group 1, 2 and 5
Authentication Mechanisms	Preshared keys
Key Management	IKE
IPSec Modes	Transport, Tunnel
IKE Modes	Main, Aggressive

Inside the customer premises, WLAN subscribers and network access to customer are authenticated based on the credentials stored locally on the network device (such as using WPA2-PSK).

Wireless LAN capabilities

The BSG model 8ew can act as a Wireless Access Point (WAP) extending the voice and data services to the Wi-Fi devices. The BSG8ew has integrated 802.11b/g access point capability that can support up to 16 users. The BSG8ew wireless access point supports following services:

- 802.11b/g WiFi interface
- QoS based on the WiFi Multimedia (WMM) specification
- Security: Open, WEP, WPA, WPA2, WPA-PSK, WPA2-PSK
- Dynamic IP address assignment to the Wireless clients - DHCP server – BSG8ew DHCP server can assign IP addresses for wireless devices.

The 802.11 frames that are received on the radio link are forwarded as 802.3 frames out the Ethernet port for further routing and forwarding. The same data services can be applied to these frames as for any other data frames. The Ethernet port of the access point can be grouped with other Ethernet ports of the BSG8ew to create a VLAN.

The WiFI Multimedia specification provides for traffic prioritization over the wireless media to ensure that users wireless connected to the BSG8ew experience similar levels of QoS as those connected to the BSG8ew with Ethernet cables.

The integrated access point does not support Connection Admission Control to reject connection requests due to insufficient bandwidth.

Monitoring and reporting

The monitoring and reporting capabilities of BSG8ew provide for collection of data that helps to monitor health of the system. The BSG8ew applications support:

- Remote Monitoring - can be used for stats, events and alarm collection, network-fault diagnosis, planning, and performance-tuning information
- SysLog (e-mail notification)
- SNMP

Solution components

This chapter describes the equipment required to implement the solution. It also describes the support services that are of interest in the context of the solution. The emphasis is however on the BSG product family. The detailed information regarding other products that are part of the solution can be obtained from corresponding documentation.

BSG8ew

BSG8ew provides a high-level security for direct connectivity to the internet service provider. In particular it provides line-rate Layer-3 IP routing, Layer-2 Ethernet switching, stateless and stateful Firewall, DHCP multi-scope server function, Network Address Translation (NAT), Virtual Private Network (VPN) application, and integrated wireless LAN support (WiFi access point), SIP-enabled Voice over IP (VoIP) proxy function with a wide range of IP Phone sets with back-ward compatibility with traditional analog telephone sets. It supports SIP ALG and NAT traversal functionality to provide for seamless traversal of voice and IPSec services across the NAT and Firewall protected interfaces.

BSG8ew is suitable for Small and Medium Business (SMB) with up to 50 users.

BSG8ew has one FE WAN interface, 7 FE LAN ports and 1 GigE LAN port. It also has 1 FXO port and 2 FXS ports to support analog sets. An integrated 802.11 b/g wireless access point extends the services of the BSG8ew to 802.11 b/g wireless laptop and handheld device.

Figure 10 – BSG8ew

LG-Nortel LIP- 6800 series IP phones

The LIP-6800 series IP Phones enable real-time voice communication over IP networks. By employing the SIP protocol, the LIP-6800 series phones interoperate with commercial soft-switch vendors products to access features and value added functionality of their hosting servers. This document describes the solution framework within which the LIP-6804 Lobby phone, LIP-6812 Desk phone, and LIP-6830 manager phone will be tested in combination with the Business Secure Gateway series, the CS2K call server, and existing Nortel SMB data products.

Figure 11 – LG-Nortel 6000 series SIP phones

Key features

- Automatic SIP registration with the host manual configuration though keys on the phone
- Password controlled web-based configuration
- Programmable flexible keys
- Power over Ethernet (PoE)
- Integrated speaker with volume control
- Volume bar providing fingertip control of audio and ringer volume settings
- Multiple line appearances
- Multiple ring-tones

LG 6000 series SIP phone key attributes

Table 6 – LG 6000 series SIP pshone key attributes

	LG-Nortel IP phone 6804	LG-Nortel IP phone 6812	LG-Nortel IP phone 6830
Key attributes			
Color	Black	Black	Black
Protocol	SIP/MGCP	SIP/MGCP	SIP/MGCP
LCD Display	N/A	3 line x 24 character LCD	3 line x 24 character LCD
Soft keys	N/A	3 Soft keys, 2 Direction keys	3 Soft keys, 2 Direction keys
LCD Contrast adjustable	N/A	Yes	Yes
Ethernet Connection	10/100, 2 RJ-45	10/100, 2 RJ-45	10/100, 2 RJ-45
Power options			
AC Power	Yes	Yes	Yes
Power Over Ethernet	Yes	Yes	Yes
Codec	G.711, G732.1A, G729AB	G.711, G732.1A, G729AB	G.711, G732.1A, G729AB
IP Protocol	TFTP, HTTPS, NTP	TFTP, HTTPS, NTP	TFTP, HTTPS, NTP
IP Address	DHCP, Static	DHCP, Static	DHCP, Static
QoS	802.1p/q, Diffserv	802.1p/q, Diffserv	802.1p/q, Diffserv
Major features			
Line Appearance	Up to 4	11	24
Shared Line Appearance	Yes	Yes	Yes
Line LEDs	Yes	Yes	Yes
Re-dial Key	Programmable	Programmable	Programmable
Flexible Keys	4	11	24
Hold Key	Yes	Yes	Yes
Mute Key	N/A	Yes	Yes
Transfer Key	Programmable	Programmable	Yes
Forward Key	Programmable	Programmable	Yes
DND Key	Programmable	Programmable	Yes
Conference Key	Programmable	Programmable	Yes
Speaker Key	OHD (Listen only)	Yes	Yes

	LG-Nortel IP phone 6804	LG-Nortel IP phone 6812	LG-Nortel IP phone 6830
Message Key	N/A	Yes	Yes
Message wait indicator	Yes	Yes	Yes
Volume Up/Down	Yes	Yes	Yes
Ringer	Yes	Yes	Yes
Handset receiver	Yes	Yes	Yes
Speaker	Yes	Yes	Yes
Headset	N/A	2.5mm jack	2.5mm jack
Wall mountable	Yes	Yes	Yes
KEM Console	N/A	Optional	Optional
Security	N/A	Yes	Yes
HTTP Secure Provisioning	Yes	Yes	Yes
Platform Compatibility: Broadsoft R14, Sylantro V3.2.1, Nortel Communications Server 2000*, Nortel Communications Server 2100*			

MCS PC client

The multimedia PC client provides advanced Internet Protocol (IP) telephony features, many of which are not available on a traditional telephone. The multimedia PC client with SIP based converged desktop service enables a user to make calls with their existing telephone, while using the multimedia PC client for multimedia services, The user answers incoming calls using their telephone. If the multimedia PC client detects that the calling party supports multimedia services, a converged desktop service call control window appears and the user can control call through that interface. Please visit respective documentation for detailed description of MCS PC client services.

IPSec VPN client

The BSG8ew is fully integrated with the SoftRemoteLT IPSec client made by SafeNet. The release 10 is the latest supported version of the client. For up to date and complete description of SoftRemoteLT supported features, visit the SafeNet documentation.

BES

BES50 series switches are equipped with a dynamic host configuration protocol (DHCP) client (configurable to BOOTP server or static IP address) and support a Web management interface compatible with the Element Manager (BEM).

- BES50FE: The BES50FE-12T PWR offers 12 full-duplex 10/100BASE-TX Fast Ethernet ports, all of which support PoE, and the BES50FE-24T PWR offers 24 full-duplex 10/100BASE-TX Fast Ethernet ports, 12 of which support PoE.
- BES50GE: The BES50GE-12T PWR offers 12 full-duplex 10/100/1000BASE-T Gigabit Ethernet ports, all of which support PoE, and the BES50FE-24T PWR offers 24 full-duplex 10/100/1000BASE-T Gig Ethernet ports, 12 of which support PoE.
- Maximum power on any port is 15.4 Watts.

BAP 120

The BAP120 is an IEEE 802.11a, 802.11b/g-compatible product that provides transparent, wireless high-speed data communications between the wired LAN and fixed or mobile devices equipped with either an 802.11a or 802.11 b/g wireless adapter, or both. Any number of BAP120 products can operate together in a network. This product can sit on a desktop or mount inconspicuously on a wall or ceiling. The BAP120 is equipped with a serial port, SNMP, and Web management interfaces compatible with the Element Manager.

General considerations

The SMB BSG8ew solution builds on the foundation of Nortel Hosted Solution Architecture that utilizes strength of the Communication Server 2000 and Multimedia Communication Server 5200 for delivery of business class voice and multimedia services. In Nortel Hosted Solution Architecture, the communication servers are located at the Nortel Hosted Solution Center and are managed by Nortel. The service provider provides for connectivity between the Nortel Hosted Solution infrastructure and SMB end users.

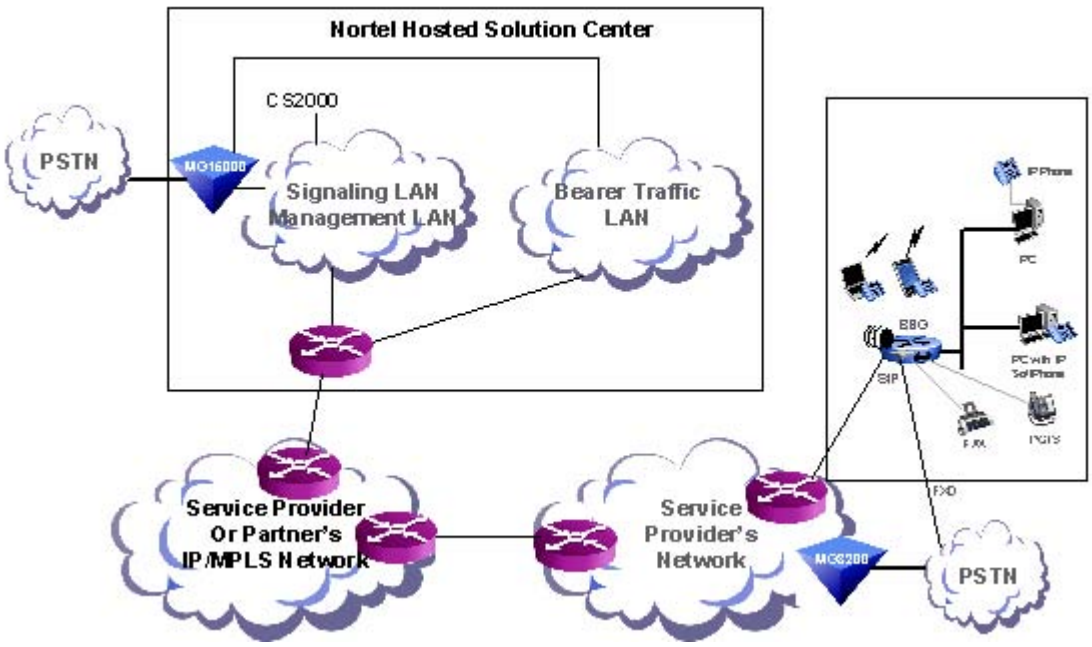
In the SMB BSG8ew solution the Business Service Gateway (BSG) is integrated with the Nortel Hosted solution architecture on one side and with the portfolio of Nortel SMB products on the other side. From the data perspective the BSG8ew is an access router that along with other customer devices constitutes customer network that is considered to be a private network. The BSG8ew is then connected to the Service Provider network, a core network, through the Service Provider edge router. From the BSG8ew solution perspective service provider core network is a public network. The service provider network needs to be capable of delivering QoS within its network to satisfy requirements of multimedia applications like voice and video. To facilitate the solution the BSG8ew is fully integrated with the SMB portfolio, see chapter Solution components (page 27) for details on the supported SMB products.

At a high level, the Hosted Solution topology consists of the core network usually managed by the service provider with the objective to provide required level of quality of service. The core network interconnects the following components of the solution:

- Communication Server (ex. CS2000)
- Service Provider Network Operation Center
- Nortel Hosted Solution Center
- Customer Access Routers with voice capabilities. For example, BSG8ew
- Internet

The network topology for the solution base architecture is presented in the following figure.

Figure 12 Nortel Hosted Solution Center



Deployment strategy

In the release 1.0 the BSG8ew solution does not provide automatic configuration of the customer premises equipment. The subsequent releases will provide such a support by means of TR-069 or SNMP applications.

In release 1.0 the BSG8ew and remaining SMB premises equipment is to be fully pre-provisioned with a functional configuration before shipping it to the site. The BSG8ew is pre configured to automatically obtain IP address for its WAN interface once installed at the customer site. It is also pre configured to allow remote management access to the box by means of HTTP/HTTPs sessions or through the SNMPv1/2/3.

Subsequent sections of this chapter describe the services configuration that aligns with this strategy. Chapter Solution components configuration example (page 95) provides detailed procedures for configuration of solution components.

Pre-configuration requirements

This section provides example of solution deployment. The section describes the sequence of events that take place during the startup process for the solution example to become operational. There are several solution components that take part in a startup process, namely BSG8ew, LG6000 phones, BES50 switch, and BAP120 access point. The sequence of events that happen during the startup process is described below.

- BSG8ew WAN interface is connected to the Ethernet port of the ADSL modem. The PPPoE client enabled on the BSG8ew WAN interface and pre-provisioned with credentials initiates handshake with the remote PPP peer to establish PPP session between the BSG8ew and the Service Provider edge router.
- The post installation configuration of the BSG8ew can be done remotely from the service providers NOC.
- The customer devices when powered up start DHCP clients on their interfaces. The DHCP requests are processed by the DHCP Server on the BSG8ew and as a result the devices are assigned IP addresses.
- LG 6800 downloads the firmware from the TFTP server. The TFTP server IP address is delivered to LG 6800 as part of DHCP OFFER in option 66 as implemented in the BSG8ew DHCP server.

To support this deployment model the following configuration requirements for the customer site equipment have to be met:

- BSG8ew pre-deployment configuration – these are the attributes that have to be configured before deployment of the BSG8ew – requires following to be pre-configured:
  - PPPoE profile (username and password) enabled for BSG8ew WAN interface
  - Reverse NAT (BSG8ew Virtual Server) and Firewall configured to allow management (HTTP/HTTPS/SNMP) sessions from MSP
  - Reverse NAT (BSG8ew Virtual Server) and Firewall configured to allow SSH/ session from MSP
  - Password changes
- BSG8ew post installation ccnfiguration:
  - TACACS+ client
  - Syslog client
  - SNTP client
  - Disabling spanning tree protocol (if only one BES is connected to the BSG8ew)
  - VLANs
  - DHCP server (address pools, option 66 for LG phones)
  - Wireless LAN
  - IPSec client termination
  - Firewall
- BES 50 fully pre configured:
  - to match customer network topology (VLANs, VLAN trunks, QoS)
  - management userID and password (other then default)
  - SNTP server the BSG8ew will use for time synchronization
  - SysLog server the BSG8ew will use to log system information
- BAP 120 fully pre configured with:
  - Country code (US or Canada)
  - UserId and password for management access (other then default)
  - SNTP server the BAP will use for time synchronization

  - — SysLog server the BAP will use to log system information
  - — Required SSIDs and security attributes
  - — Mapping of SSIDs to VLANs as per functional requirements
  - — DHCP client enabled
- LG 6800 phones pre configured with
  - — DHCP client enabled (requests the TFTP server IP address through option 66)
  - — The IP address of the proxy server (another option is to add it to the LG configuration file located on the TFTP server)

BSG8ew interfaces

In a default configuration the BSG8ew model has one WAN interface and 8 LAN interfaces that can be used to connect customer devices. Both WAN and LAN interfaces are Ethernet based. In the solution the Ethernet ports are grouped to form VLANs, see LAN interfaces (page 37).

The BSG8ew can be viewed as a gateway that interconnects customer network with the outside world. It provides routing capabilities between the VLANs themselves and between the VLANs and WAN interface.

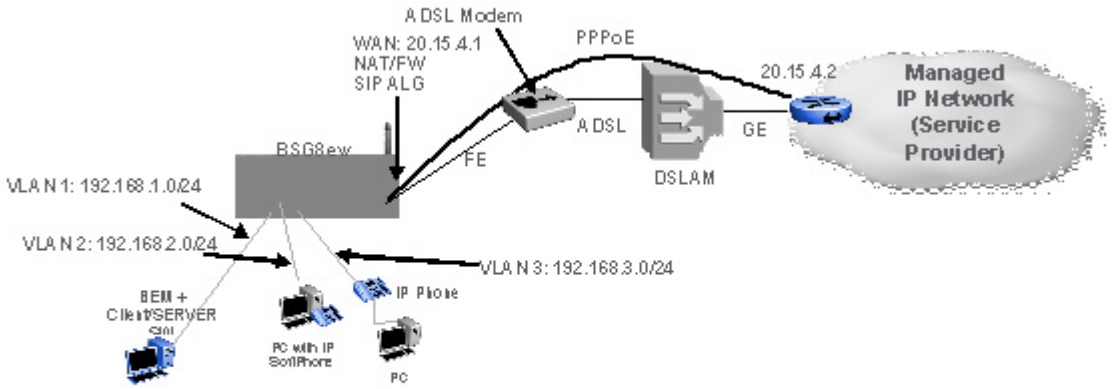
The DHCP server is enabled for VLAN interfaces for dynamic assignment of the IP addresses. A DHCP client is by default enabled for WAN interface to dynamically obtain IP address from the service provider. Once the IP addresses are assigned the traffic from the customer devices can be routed out the WAN interface subject to the NAT and Firewall policies.

WAN interface

To connect the BSG8ew to the service provider network the WAN Ethernet port is connected to a WAN access device. The WAN access device can be a DSL or cable modem or it can be another router or switch Ethernet port with the WAN connectivity to the service provider network. Figure 13 BSG8ew WAN connectivity (page 37) describes BSG8ew WAN connectivity with the use of ADSL modem. In this case the BSG8ew needs to be configured with the PPPoE client and with the credentials to match the authentication requirements of the service provider network.

The BSG8ew implements the rate limiting feature that allows programming available bandwidth on the WAN interface. This is useful when using low speed WAN links like DSL modems. Rate Limiting feature matches the bandwidth of WAN interface with the available uplink bandwidth of the DSL link.

Figure 13 BSG8ew WAN connectivity



LAN interfaces

The ports on the BSG8ew can be grouped into three VLANs effectively partitioning the network into separate broadcast domains. Each VLAN is represented by the separate Virtual Interface. The traffic between the VLANs can only be routed. The solution partitions the customer network into three VLANs designated as follows:

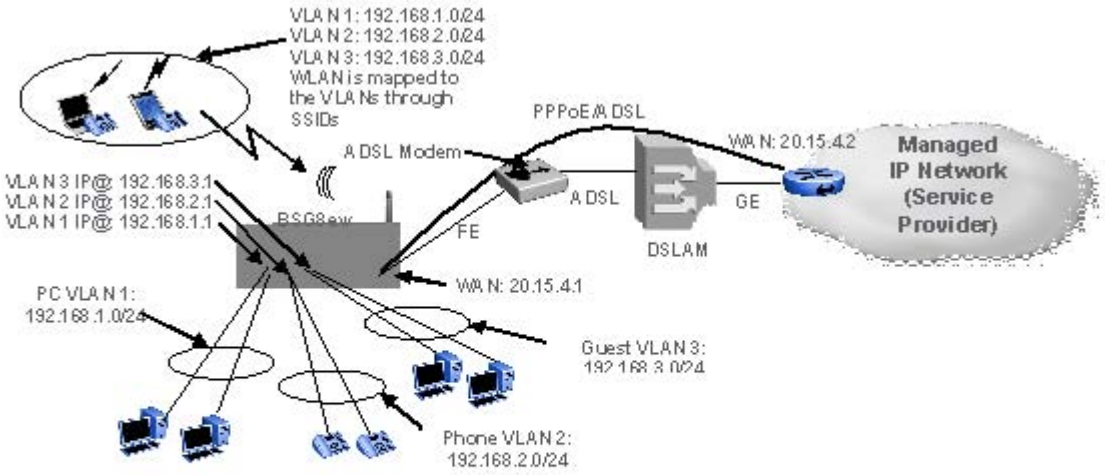
- VLAN 1: This is a VoIP VLAN, only IP phones can be connected to the ports that are members of this VLAN
- VLAN 2: This is a Data VLAN, all devices other then IP phones should be connected to this VLAN
- VLAN 3: This is a Guest VLAN; devices on this VLAN do not have access to VLAN 1 and VLAN2; they are allowed connectivity only to the Internet
- The BSG8ew has 8 Ethernet ports available for LAN/VLAN connectivity. Ports 1 through 7 are Fast Ethernet ports and port 8 is a Gigabit Ethernet port. In the solution, the six FE ports are partitioned into three VLANs and assigned IP addresses as follows:
- Ports 1 and 2: VLAN 1 with virtual interface IP address of 192.168.1.1 and mask 255.255.255.0
- Ports 3 and 4: VLAN 2 with virtual interface IP address of 192.168.2.1 and mask 255.255.255.0
- Ports 5 and 7: VLAN 3 with virtual interface IP address of 192.168.3.1 and mask 255.255.255.0

The Gigabit Ethernet port is pre-provisioned as trunk port with three VLANs. This facilitates automatic expansion of the customer network in case number of BSG8ew ports is too low to meet the customer needs.

Nothing precludes the customer from changing port assignments if such a need arises.

The external traffic, from the WAN interface is routed to the VLAN devices by means of the Virtual Interface IP address. There is a single virtual interface IP address assigned to the VLAN interface meaning that all the devices connected to the ports that constitute the VLAN are in the same subnet. The described configuration is presented in the following figure.

Figure 14 Base customer network partitioning using VLANs



LAN to WAN routing

In order to enable LAN to WAN routing several things need to happen:

- Customer device, phone or PC in Figure 14 Base customer network partitioning using VLANs (page 38), needs to obtain IP address (DHCP server has to be enabled on the LAN/VLAN interface and it has to have IP address pools configured) along with the default gateway (ex. 192.168.1.1 for VLAN 1 devices).
- BSG8ew's WAN port needs to obtain IP address from the Service Provider (DHCP Client needs to be enabled on the WAN port).
- Firewall filters and Firewall access lists need to be provisioned to allow traffic between LAN and WAN ports.
- NAT needs to be enabled for LAN to WAN translation.

IP address allocation

The BSG8ew allows for both static and dynamic allocation of IP addresses to both its WAN and LAN interfaces. In the solution, if the BSG8ew WAN connectivity is over the PPPoE tunnel. The IP address of the WAN interface is dynamically obtained from the PPPoE server during PPP network control protocol negotiation. The three VLANs defined in the solution (as per section 3.3.2) have DHCP server enabled. The devices on these VLANs are served by the DHCP server that has three address pools configured for the networks as follows:

- 192.169.1.0/24 for VLAN 1
- 192.168.2.0/24 for VLAN 2
- 192.168.3.0/24 for VLAN 3

SSID to VLAN mapping

The BSG8ew integrated access point aggregates the traffic from Wi-Fi devices. As part of the solution the Wi-Fi devices are also partitioned into three SSIDs that in turn are mapped to three VLANs defined on the BSG8ew. It is recommended that Wi-Fi stations equipped with SIP soft phones associate with the SSID dedicated for voice usage which internally maps to VLAN 1, wireless stations that will be primarily sending only data traffic associate with data SSID mapped to VLAN 2 and guest access is available through the Guest SSID mapping to VLAN 3. The Wi-Fi devices are assigned to the specific VLAN by mapping the device SSID to the VLAN Id. For example there will be three SSIDs, one per device type:

- SSID 1 maps to VLAN 1 (voice)
- SSID 2 maps to VLAN 2 (data)
- SSID 3 maps to VLAN 3 (guest)

The packets received at the BSG8ew access point and mapped to the particular VLAN receive the same treatment along the data path in the BSG8ew as packets in that VLAN received on non WiFi interface. They are subject to the same security and QoS requirements. They are also dynamically assigned IP addresses from the DHCP address pool that corresponds to the VLAN they belong to.

End-to-end Quality of Service

Since the BSG8ew solution delivers both voice and data services it is mandatory that the end-to-end QoS is present. There are two distinct domains where the QoS is required. These are the Service Provider QoS domain and the SMB customer QoS domain. They can both follow diffServ architecture as presented in Figure 15 End-to-end diffServ domain (page 40). In this case diffServ domain extends end to end and QoS is managed at L3. Or the SMB QoS is implemented as 802.1p at L2 and service provider is in a diffServ domain. In this case there is a need to map the 802.1p domain to the DiffServ domain to ensure proper quality of service. This second option is presented in Figure 16 DiffServ domain in the core network and 802.1p in the customer network (page 40). ___

Figure 15 End-to-end diffServ domain

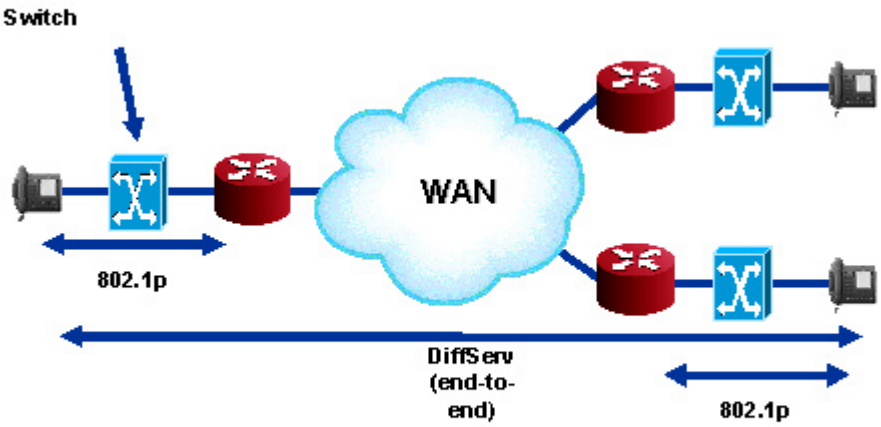
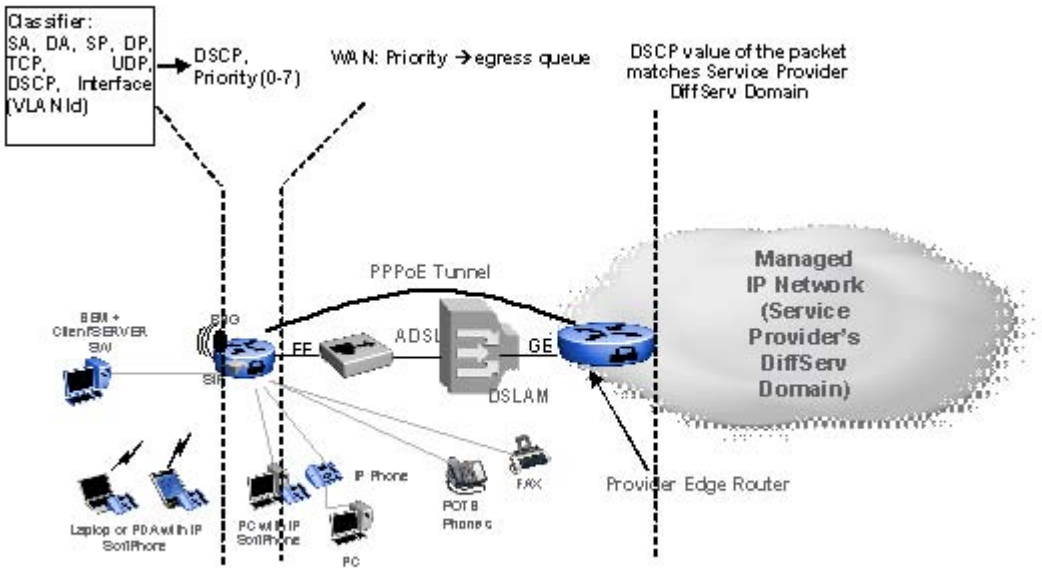


Figure 16 DiffServ domain in the core network and 802.1p in the customer network

The service provider QoS domain is a responsibility of the service provider and the mechanisms it deploys depend on the type of the Service Provider network. The SMB QoS domain is mainly enforced by Business Services Gateway and the interconnected SMB devices that constitute the customer network. Although the two domains are independent and they can deploy different QoS schemes they have to be implemented so the end-to-end QoS level can meet the requirements. The packets that are considered to be high priority in SMB network, like voice packets, also have to be treated as high priority packets in the service provider network.

The assumption is that the service provider network is itself the diffServ domain so it can use the information carried in the DSCP field of the IP header of the packet to prioritize the packets accordingly. The BSG8ew can mark or re-mark DSCP value of the packets that are going towards the service provider network to match the service provider diffServ schema. This ensures proper QoS treatment for the customer packets when traversing service provider network. As presented in Figure 17 802.1p to DSCP mapping (page 41), packets originated at the customer device are first classified in the ingress direction on the BSG8ew then before transmitting the packet out the WAN interface IP header is set with the DSCP value that matches service provider diffServ domain. The packet is also assigned the priority that corresponds to its traffic type. Based on the priority assigned to the packet the egress queue is selected when transmitting the packet through the WAN interface.

Figure 17 802.1p to DSCP mapping



To facilitate classification and resulting prioritization of the voice packets incoming on the LAN interface the BSG8ew solution recommends grouping the IP phones and other devices in different VLANs as presented in Figure 14 Base customer network partitioning using VLANs (page 38). This allows separation of the traffic type per VLAN and provides for traffic classification based on the VLAN Id or corresponding subnet and assigning PHB according to the requirements of the traffic type.

The network partitioning based on the traffic type is not always possible one example being a soft phone application. In this case it is not possible to separate the voice traffic from data traffic by means of VLAN and the solution is to use soft-phone application that is capable of marking voice packets with the required diffServ code point.

The common customer configurations and respective QoS solutions are presented in sections IP phones connected directly to the BSG8ew LAN port (page 48) through QoS implementation for PC soft phone (page 51).

The base solution QoS design follows Nortel recommendation. The signaling traffic is to be marked with the DSCP PHB of CS5. The VoIP media traffic (RTP) is to be marked with the PHB of EF. Both SIP signaling and VoIP traffic is to be queued onto the highest priority queue with the strict priority scheduler. The table Elasti categories and corresponding PHBs (page 43) summarizes PHB assignment based on the traffic characteristics.

Elasti categories and corresponding PHBs

Application Service Class	Elasticity	DHCP	Loss	Delay	Jitter
Network Control	both	CS6	Low	Low	--
Telephony	inelastic	EF	Very Low	Very Low	Very Low
Real-Time Interactive	inelastic	CS4	Low	Very Low	Low
Multimedia Conf	rate adaptive	AF4x	Low/Med	Very Low	Low
Signalling	inelastic	CS5	Low	Low	--
Broadcast Video	inelastic	CS3	Very Low	Med	Low
Multimedia Streaming	elastic	AF3x	Low/Med	Med	--
Low Latency Data	elastic	AF2x	Low	Low/Med	--
High Throughput Data	elastic	AF1x	Low	Med/High	--
OAM	elastic	CS2	Low	Med/High	--
Standard	both	DF	Not specified	Not specified	--
Low Priority Data	No spec	CS1	High	High	--

Service based QoS requirements/DSCP marking

Today data networks provide transport infrastructure that carries types of traffic with different QoS requirements in terms of jitter, delay and loss of the packets. Various types of traffic and corresponding requirements are presented in Elasti categories and corresponding PHBs (page 43). QoS mechanisms are designed to facilitate the needs of various types of traffic in terms of their traffic characteristics.

The BSG8ew solution recommendation is to follow Nortel QoS recommendation for Nortel Networks class of service definitions when mapping services to diffServ code points.

The following DiffServ code points should be used for identification of the different packet flows that make up the telephony service. The values provide here follow Nortel recommendations for QoS requirements.

DSCP Marking for voice signaling and media traffic

- CS5 DSCP value should be used for SIP signaling packet flows between the SIP call server located at the Hosted Solution Center and the BSG8ews SIP proxy server.
- EF DSCP value should be used for voice media packet flows between the SIP phones connected through the BSG8ew to the Service Provider Network. The summary of the described diffServ marking requirements are presented in Table 8 – Applications and corresponding PHBs (page 44).

Table 8 – Applications and corresponding PHBs

Traffic Category	NNSC	Application Example	DHCPs in NNSC
Network Control	Critical	Critical Heartbeats	CS7
	Network	Routing	CS6
interactive	Premium	IP Telephony	EF, CS5
	Platinum	Video Conference	AF4x, CS4
Responsive	Gold	Streaming Media	AF3xAF4x, CS3
	Silver	Client / Server	AF2xAF4x, CS2
Timely	Bronze	Store and Forward	AF1xAF4x, CS
	Standard	Best Effort	DF (CS0)

Attention: X = 1, 2, or 3 and CS0 has a DSCP value of 000000 and is equivalent to the DF DSCP. Both CS0 and DF use the same DF PHB.

BSG8ew default DSCP to 802.1p mapping

The BSG8ew is pre programmed with the default mapping of the diffServ code points to the IEEE 802.1p priority bit. The scheduling algorithms for traffic queues are also pre programmed. The mappings are presented in Table 9 – Default DSCP to 802.1p mapping (page 45).

Table 9 – Default DSCP to 802.1p mapping

DSCP	Queue Number	NNSC	Scheduler	Maps to 802.1p
CS7	0	Critical	1st Strict	7
CS6	0	Network	1st Strict	7
EF, CS5	1	Premium	2nd Strict	6
AF41, AF42, AF43, CS4	2	Platinum	3srd Strict	5
AF31, AF32, AF33, CS3	3	Gold	WRR	4
AF21, AF22, AF23, CS2	4	Silver	WRR	3
AF11, AF12, AF13, CS1	5	Bronze	WRR	2
DF, CS0, all undefined DSCPs	7	Standard	WRR	0

The default mappings are designed to ensure that the requirements of different traffic types in terms of delay, jitter and packet loss will be met. It should be noted that the mapping will result in correct QoS treatment only if the DSCP value of the packet received on the WAN interface is as per Table 9 – Default DSCP to 802.1p mapping. If this is not the case and Service Provider DiffServ domain does not match the BSG8ew's default DSCP settings, the mapping should be changed accordingly.

Egress queue setting

There are eight egress queues per port available on BSG8ew for egress traffic prioritization. These queues are directly mapped to the 8 classes of service. Mapping of 802.1p priority bits to egress queue is hard wired and it is as follows:

Egress Queue = 7 - 802.1p Priority

There are two scheduling algorithms available to serve the queues, strict priority scheduling and waited round robin scheduling. It is important to have the correct scheduling algorithm assigned to the queue based on the type of the data it is used for. Nortel recommends using Strict Priority scheduling for queue used for time critical and delay sensitive traffic such as voice, both signaling and media packets, and WRR for any other type of traffic.

The scheduling algorithms are presented in Table 9 – Default DSCP to 802.1p mapping (page 45).

VLAN to WAN or VLAN to VLAN QoS implementation

Following the customer network topology as presented in section LAN interfaces (page 37) the BSG8ew VLAN interfaces can receive packets from three different VLANs with the following characteristics:

- Traffic received from the devices on VLAN 1. This is voice signaling and media traffic. The signaling traffic can be classified based on the destination port of 5060 (SIP well known port). This is employee voice traffic that should be treated with priority higher then employee data and guest traffic.
- Traffic received from the devices on VLAN 2. This is employee data traffic and employee voice (signaling and media) traffic if the PC is running SIP soft-phone.
- Traffic received from devices on VLAN 3. This is guest traffic and it should be treated with the lowest priority comparing to the VLAN 1 and VLAN 2 traffic.

The classification of the ingress frames can be done on any of the supported field (as per section Data services (page 20). For the purpose of the configuration presented in this document source network address or VLAN id and destination port can be used to classify and prioritize the traffic.

Based on the above network topology and corresponding traffic characteristics the packets that are received on the VLAN Interfaces are processed as follows:

- Packets are classified based on the VLAN Id and source/destination port
- packets that match VLAN Id 1 and port 5060 are marked with the DSCP value of CS5 and assigned priority 6 (to be send to strict priority queue)
- packets that match VLAN Id 1 and do not match port 5060 are marked with the DSCP Value of EF and are assigned priority 6 (to be send to strict priority queue)
- packets that match VLAN Id 2 and DSCP value of CS5 (voice signaling packets) are assigned priority 6 and DSCP value is not changed
- packets that match VLAN Id 2 and DSCP value of EF (voice media packets) are assigned priority 6 and DSCP value is not changed
- packets that match VLAN Id 3 are assigned priority 0 and DSCP value is set to DF to make sure that they do not compete wit the voice traffic of VLAN 1 and VLAN 2
- This process is also valid for packets received from Wi-Fi devices that are associated with the BSG8ew's integrated Wireless Access Point

1.4.5 WAN to VLAN QoS implementation

In a WAN to LAN direction, the default BSG8ew DSCP to 802.1p mapping as per Table 9 – Default DSCP to 802.1p mapping (page 45) is used. The mapping can be changed to align it with the DiffServ domain of the Service Provider network if such a need exists. The BSG8ew allows setting the 802.1p bit and priority of the packet based on the DSCP value of the packet.

1.4.6 WLAN QoS

The packets from the wireless devices are crossing two QoS domains before they are transmitted out the interface. First, they are subject to over the air QoS and then as any other packet they are subject to BSG8ew QoS framework. The BSG8ew Wireless Access Point supports over the air QoS as per WMM specification. However to utilize the WMM support the application needs to be capable of inter working with the WMM layer. The default WMM settings on the BSG8ew are presented in Table 10 – WMM 802.1D priority to access class mappings (page 47).

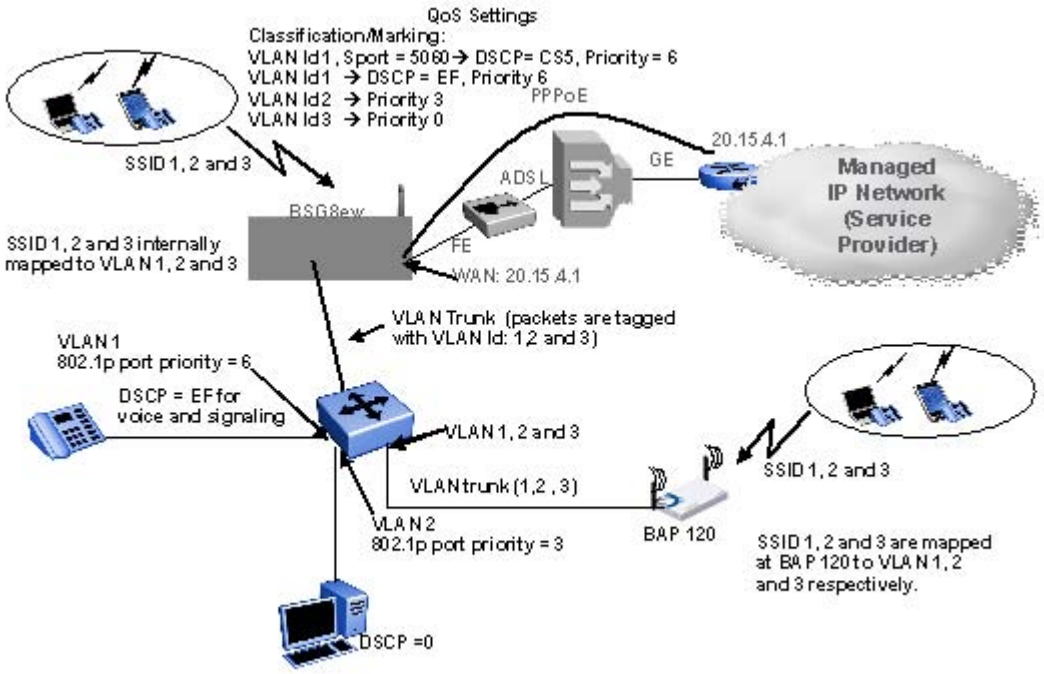
Table 10 – WMM 802.1D priority to access class mappings

Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation
lowest	1	BK	AC_BK	Background
	2	-		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
highest	7	NC		

The packets received on the WiFi interface are mapped to the VLANs based on the SSID. Once the packet is tagged with the specific VLAN ID the BSG8ew QoS mechanisms can be applied as for any non WiFi originated packet. This is illustrated in Figure 18 WLAN QoS implementation.

The packet corresponding to SSID 1 is tagged with VLAN Id 1 at the BAP 120 or is internally mapped to VLAN ID 1 if it is received on the BSG8ew integrated Access Point. The packet can be classified based on the corresponding VLAN Id and marked with the DSCP value and priority (egress queue) accordingly.

Figure 18 WLAN QoS implementation


QoS Settings
Classification/Marking:
VLAN Id1, Sport = 5060 → DSCP= CS5, Priority = 6
VLAN Id1 → DSCP = EF, Priority 6
VLAN Id2 → Priority 3
VLAN Id3 → Priority 0
PPPoE
20.15.4.1
GE
ADSL
SSID 1, 2 and 3
BSG8ew
SSID 1, 2 and 3 internally mapped to VLAN 1, 2 and 3
FE
WAN: 20.15.4.1
Managed IP Network (Service Provider)
VLAN Trunk (packets are tagged with VLAN Id: 1,2 and 3)
VLAN 1
802.1p port priority = 6
DSCP = EF for voice and signaling
VLAN 1, 2 and 3
VLAN trunk (1,2, 3)
SSID 1, 2 and 3
VLAN 2
802.1p port priority = 3
BAP 120
SSID 1, 2 and 3 are mapped at BAP 120 to VLAN 1, 2 and 3 respectively.
DSCP =0

IP phones connected directly to the BSG8ew LAN port

In a small scale deployment customer devices are directly connected to the BSG8ew Ethernet ports. There is no intermediate switch between the BSG8ew and the customer devices. This configuration is presented in Figure 19 IP phones connected directly to the BSG8ew LAN port (page 49). As per Nortel recommendation, both voice bearer (RTP) and signaling (SIP) packets need to be queued onto priority 6 egress queue. In the example in Figure 19 IP phones connected directly to the BSG8ew LAN port ports and 802.1p priorities are assigned as follows:

- Voice VLAN (1) Port 1 and 2: priority 6
- Data VLAN (2) Ports 3 and 4: priority 3
- Guest VLAN (3) Ports 5 and 6: priority 0

The packets received on the BSG8ew switch ports are prioritized based on the VLAN Id and the source port. In our example the packets received from the IP phones are sent to the priority 6 queue, from data PC to the priority 3 queue and from the guest PC to the priority 0 queue. Thus the voice packets will always take precedence over data and guest packets when transmitting out the WAN interface.

Before the packets are sent out they must have the correct DSCP value in their IP header. The BSG8ew can not classify packets based on the protocol type other then TCP or UDP. The solution is to classify the signaling packets based on the well known port number 5060 used by SIP protocol. Anything else that does not use port 5060 is the media traffic. Thus for the network configuration as presented in Figure 19 IP phones connected directly to the BSG8ew LAN port (page 49) the QoS settings would be as follow:

Classifier 1: VLAN ID = 1, Source Port = 5060

Packet Marking: DSCP = CS5 (SIP signaling)

Packet Priority: 6

Classifier 2: VLAN ID = 1 Source Port = any

Packet Marking: DSCP = EF (RTP)

Packet Priority: 6

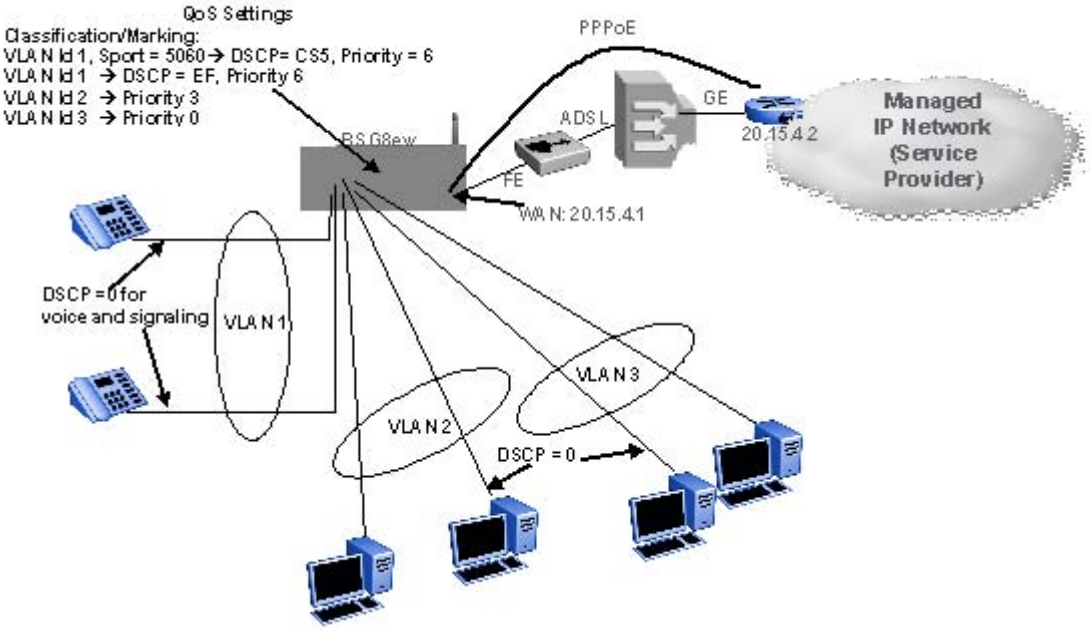
Classifier 3: VLAN ID = 2

Packet Priority: 3

Classifier 4: VLAN ID = 3

Packet Priority: DF (0)

Figure 19 IP phones connected directly to the BSG8ew LAN port



IP phones connected to the L2 switch

In a larger scale deployment the customer devices are not directly connected to the BSG8ew but rather to the L2 switch that itself is connected to the Ethernet port of the BSG8ew. In the example in Figure 20 IP phones and PCs connected to the switch (page 50) the BES50 is connected to port 7 of the BSG8ew. Similarly to previous configuration the customer network is partitioned into

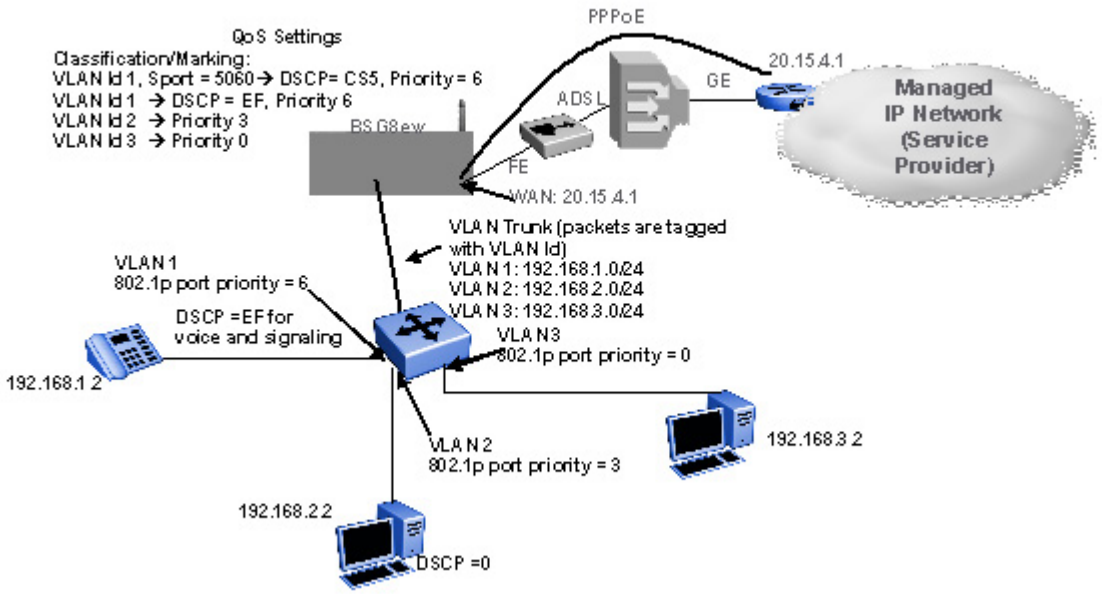
three VLANs. VLAN 1 contains IP Phones, VLAN 2 contains PCs and VLAN 3 is a guest VLAN. There is a VLAN trunk configured between the port 7 of the BSG8ew and corresponding port on the BES50. The VLAN trunk carries traffic from the three VLANs that constitute the customer network: Voice VLAN 1, Data VLAN 2, and Guest VLAN 3.

In this configuration QoS must be applied on both BES50 and BSG8ew interfaces. The voice traffic originated in VLAN 1 has a higher priority then the data traffic form VLAN 2 and VLAN 3. In this example the BES50 ports for VLAN 1 are configured with priority 6, VLAN 2 with priority 3 and VLAN 3 with priority 0. The packets received on these ports will be tagged with 802.1p priority corresponding to the port priority. That priority is then used in egress direction when transmitting the packet out the VLAN trunk towards the BSG8ew port 7.

The appropriate scheduling algorithm should be applied to egress queues on both BSG8ew and BES ports. Both BSG8ew and BES50 support strict priority and WRR scheduling algorithms. The recommended scheduling algorithm is provided in Table 9 – Default DSCP to 802.1p mapping (page 45).

Similarly to example in section IP phones connected directly to the BSG8ew LAN port (page 48), the BSG8ew can classify and prioritize the traffic received from BES50 across the VLAN trunk based on the VLAN ID of the packet.

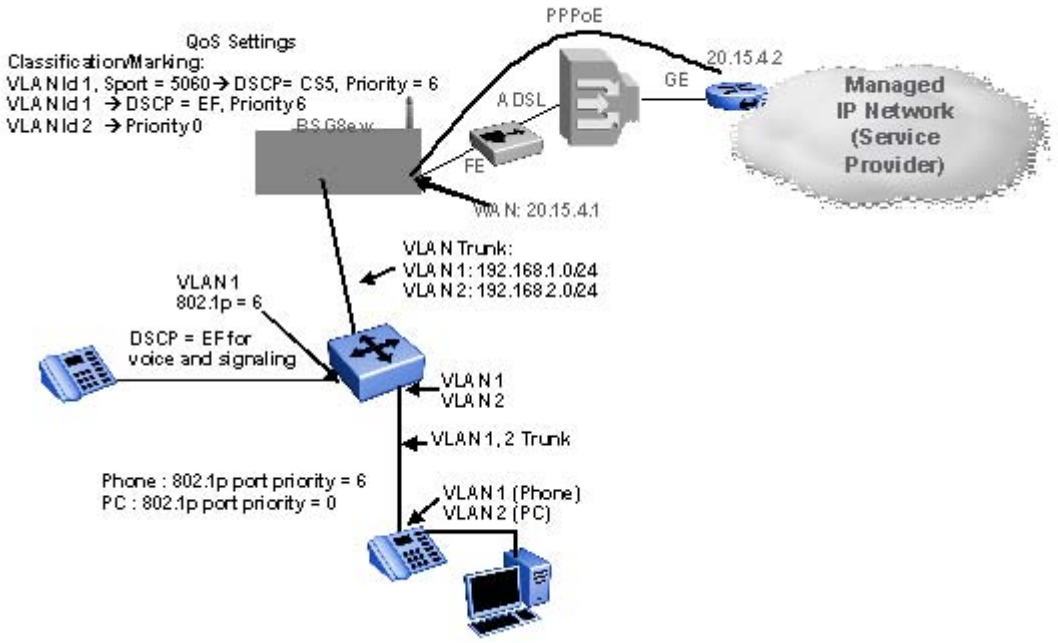
Figure 20 IP phones and PCs connected to the switch



IP Phone and PC share the same L2 switch port

When the PC is connected to the network through the IP phone switch port the voice traffic and the data traffic from the PC can be separated by defining two VLANs on the IP phone network port. This configuration is presented in Figure 21 IP phone and PC share the same switch port. The VLAN trunk between the IP phone port and the switch port separates the voice signaling and media packets from the PC data packets.

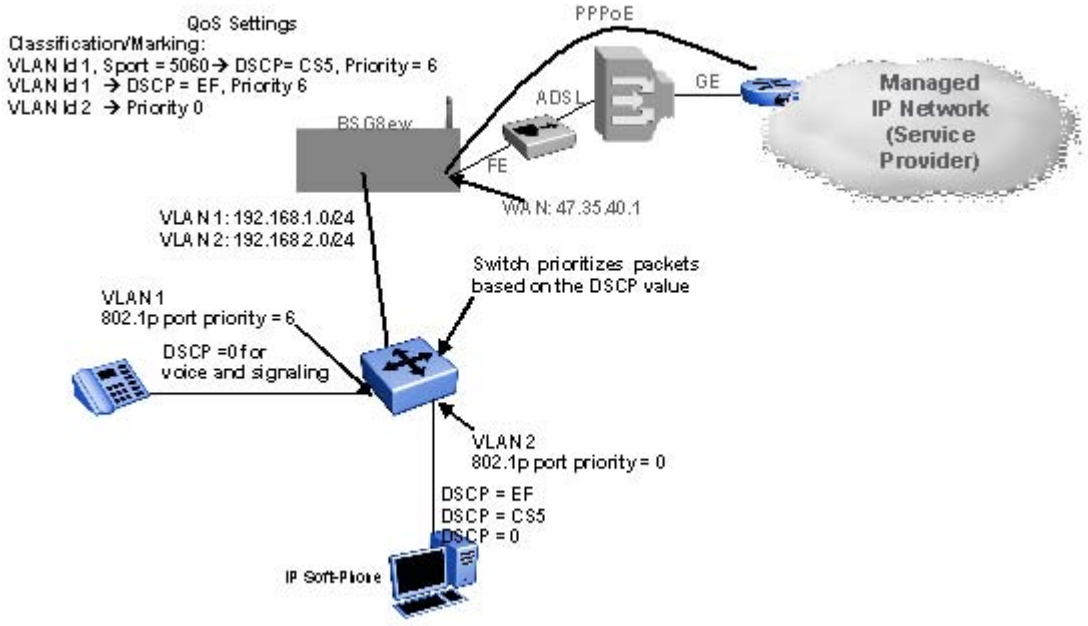
Figure 21 IP phone and PC share the same switch port



QoS implementation for PC soft phone

The port prioritization can not be used to prioritize the traffic for PC Soft Phone because the PC can have applications that require different priority than for VoIP. To prioritize the voice traffic from the PC soft phone the soft phone application has to be capable of marking the voice packets with the required DSCP value. If the L2 switch is DSCP aware the voice packets received from the PC with the soft phone application can be prioritized on the L2 switch based on the DSCP value in the IP header. BES family switches are capable of prioritizing packets based on the DSCP value in the IP header. The described process is presented in the following figure.

Figure 22 IP Soft phone QoS



Security

The BSG8ew is a gateway between the customer network and the external world. In the solution the assumption is that the BSG8ew WAN interface is a public interface and the access over this interface should be controlled. Access to the LAN interfaces can also be controlled through authentication and firewall.

To facilitate network security, the BSG8ew provides a number of features to meet different security requirements such as secure management access, stateful and stateless firewall, Intrusion Detection System (IDS)/Intrusion Protection System(IPS), Application Layer Gateway (ALG), support for network address translation (NAT), VPNs, 802.1x access control.

Secure management access

In the reference architecture the network management station or NMS resides outside the customer premises. It is therefore paramount to secure the management traffic since it often must traverse an un-trusted domain (e.g. the Internet). BSG8ew provides HTTPS, SSH, and SNMPv3 secure management protocols to access the device remotely to perform OAM functions.

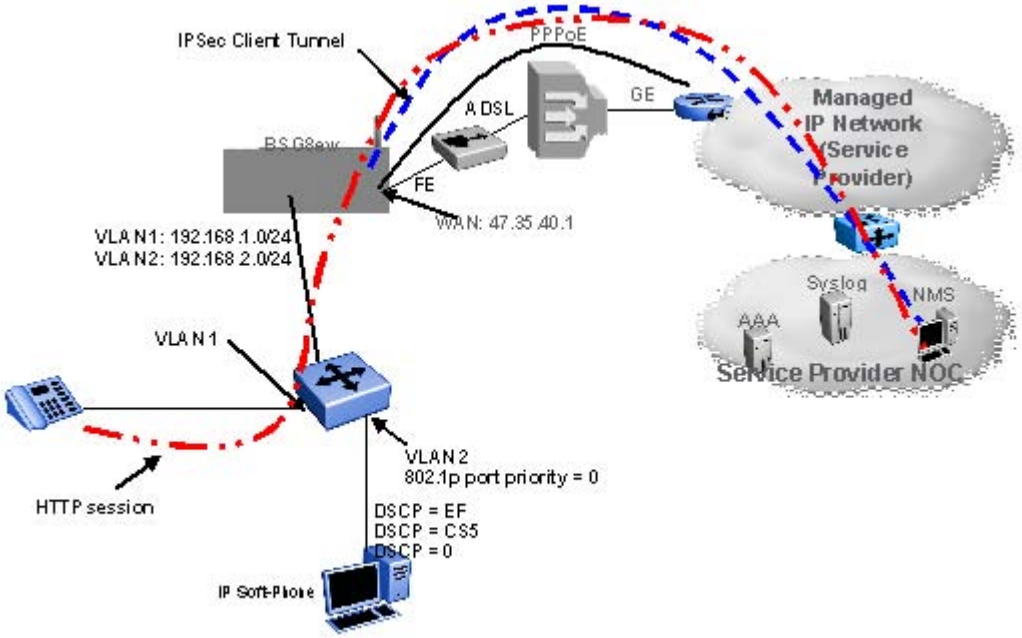
For remote management, the BSG8ew firewall must be configured to let these management protocols pass through from the WAN side.

Unsecured protocols such as HTTP, Telnet, and SNMP v2c should be used when initiated from the LAN or if this protocols can be secured by some other means for example over an IPSec tunnel.

For secure management access to the customer devices on the private LAN IPSec client tunnel needs to be established between the management station and the BSG8ew. The Telnet, HTTP or SNMP session can then be established with the device of interest. The Telnet, HTTP or SNMP packets will be tunneled through the IPSec client tunnel and routed by BSG8ew to the destination device. This configuration is presented in Figure 23 Secure management access to customer devices (page 53).

If no secure management access is required the BSG8ew can be configured to allow the administrator telnet access through any of the LAN interfaces from its CLI command line.

Figure 23 Secure management access to customer devices



NAT, Firewall, and ALG

The BSG8ew supports both stateless and stateful firewall. The stateless firewall is an Access Control List. In the solution the stateful firewall is applied for WAN to LAN direction. No firewall is applied to traffic within a trusted interface for example LAN to LAN traffic, with exception of the Guest VLAN. The traffic originated from the devices on the Guest VLAN is controlled by Access Control List to ensure that it can not access customer voice or data VLANs, VLAN 1 and VLAN 2.

The BSG8ew has by default dynamic NAT enabled on the WAN interface. Any packet received on a LAN interface and routed out the WAN interface has its source address replaced with the IP address of the WAN interface before sending it out. The presence of NAT on the WAN interface hides the IP addresses of the customer network and makes them inaccessible outside of the session originated from within the customer network.

From security perspective, both NAT and Firewall are desirable, they protect customer network from unauthorized access. They may however cause issues for services like voice.

To ensure smooth operation of voice services across the NAT and Firewall BSG8ew implements the SIP Application Layer Gateway (ALG). The SIP ALG manipulates the private IP addresses in outgoing SIP messages to public IP addresses for facilitating NAT traversal. It creates necessary mappings within the NAT module for signaling and media flows and also opens pinholes in the firewall.

The SIP ALG is automatically enabled if NAT is enabled on the WAN interface. There is no provisioning required to enable SIP ALG.

Authentication

In the reference architecture, the service provider is responsible for managing the network devices including BSG8ew. It is recommended to use centralized authentication server for administrator access to the BSG8ew, in particular when the service provider has a large number of sites to manage.

The customer devices can be authenticated locally at the BSG8ew or through central authentication server that could be RADIUS or TACACS.

The description of authentication methods is provided below.

Logging authentication

The users logging into the BSG8ew can be authenticated based on the credentials stored in the local database or at the central database by means of TACACS+ RADIUS protocols. The centralized authentication may often be preferred option for scalability reasons.

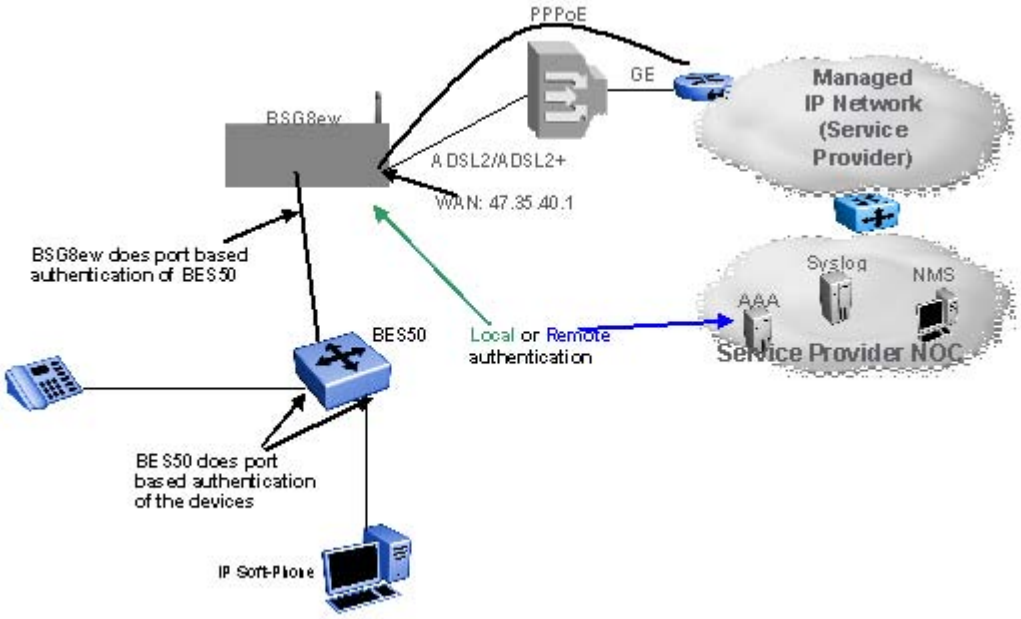
The BSG8ew allows fall back to local database in case the TACACS or RADIUS server is not available.

Port based authentication (authentication of VLAN ports)

The BSG8ew supports authentication of the devices that are connected to its VLAN ports in order to permit the device to access the port. BSG8ew authenticates the user by means of 802.1x Port Based Access Control protocol and it supports both local and remote authentication using RADIUS.

The port based authentication authenticates the device connected to the port. In case when there is a L2 switch connected to the BSG8ew LAN port the port based authentication process authenticates the switch only. The devices that are connected to the switch must be authenticated by the switch. Otherwise they transparently get access to the network simply because they are connected to the switch that has been authenticated. If the switch does not authenticate connected devices an 802.1x MAC based authentication mode (see section below) should be enabled on the BSG8ew to ensure that only authorized devices get access to the network.

Figure 24 Port based authentication

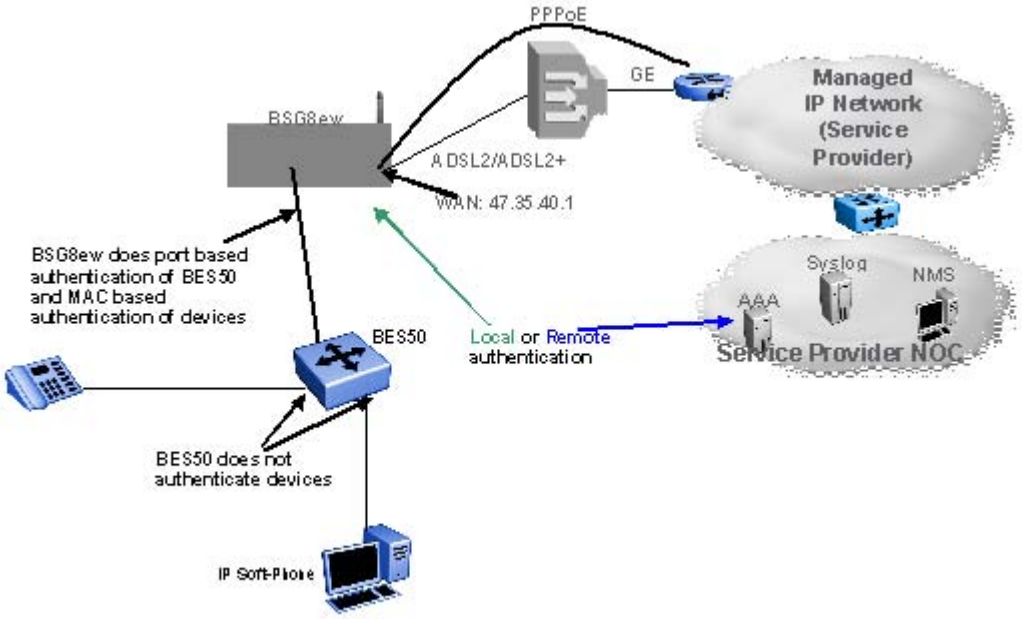


MAC based authentication

In addition to port based authentication the BSG8ew supports 802.1x MAC based authentication. The MAC based authentication can be used to authenticate devices that are not directly connected to the BSG8ew port but rather to the switch port that is connected to the BSG8ew port. The switch in this case does not authenticate the devices but lets the BSG8ew authenticate the devices based on the MAC address of the device. This configuration is presented in Figure 25 Mac based authentication (page 56) below.

The 802.1x authentication mode is by default set to port based authentication.

Figure 25 Mac based authentication



Authentication of Wi-Fi devices

Every Wi-Fi device has to be authenticated before permission to access the network is granted. Inside the customer premises, WLAN subscribers and guests with network access can be authenticated based on the credentials stored locally on the network device (such as using WPA2-PSK) or they can be authenticated through the remote AAA server by means of 802.1x framework. The BSG8ew supports RADIUS for network access authentication.

The complete set of supported authentication options is provided in the following table.

BSG8ew Wi-Fi security protocolsBSG8ew Wi-Fi security protocolsBSG8ew Wi-Fi security protocolsBSG8ew Wi-Fi security protocolsBSG8ew Wi-Fi security protocols

Authentication	**Cipher**
WPA (Enterprise)	TKIP
WPA-PSK (Personal)	TKIP
WAP2 (Enterprise)	AES-CCMP
WPA2-PSK (Personal)	AES-CCMP

Authentication of the user with the SIP call server

The SIP phones require to be authenticated by the SIP call server at the Hosted solution center to get access to call services. The SIP phone will have to be configured with the user credentials that correspond to the user account on the central call server:

- user name
- password

SIP clients are not authenticated by BSG8ew SIP proxy. They are entered into the BSG8ew registrar database after they have been authenticated by the external SIP server.

Customer network partitioned into VLANs

Traffic within the customer premises network can be separated into multiple virtual LANs (VLANs) to prevent traffic flow between end devices that have different security requirements. For example, separate guest access from employee access. If VLAN traffic separation is required, Nortel recommends the following VLAN configuration:

Table 12 – VLAN descriptions

VLAN 1 and Native	Voice over IP traffic
VLAN 2	Management and data traffic
VLAN 3	Guest traffic

Devices in the guest VLAN can only access external network (e.g. Internet) through the BSG8ew WAN interface, subject to the security policy imposed by the customer premises network administrator. The BSG8ew firewall must be configured to prevent guests from accessing the voice and data VLAN.

Service availability

There are two aspects of BSG8ew in terms of service availability. The data services aspect and the voice services aspect. In the context of this document the data services aspect is relevant only if it provides for increased availability of the voice services. The BSG8ew supports VRRP protocol that increases service availability at the data services layer. It does not however increase the availability of the voice services and as a result it is not discussed here.

Call routing to the PSTN network

In a normal mode of operation when the central SIP call server is available calls from all the devices, including FXS endpoints are handled as VoIP calls and are routed to the data network.

If the central SIP call serve becomes unavailable the BSG8ew switches to the backup mode and the calls are routed as per backup dialing plan. For example the backup dialing plan can be configured to route the calls to the PSTN network through the FXO interface.

The emergency calls, for example. 911 calls take precedence over non-emergency calls when routed out to the PSTN network through FXO interface. If there is non-emergency call active on the FXO interface and emergency call is received on that interface, the non-emergency call is terminated.

BSG8ew backup mode in case of WAN interface failure

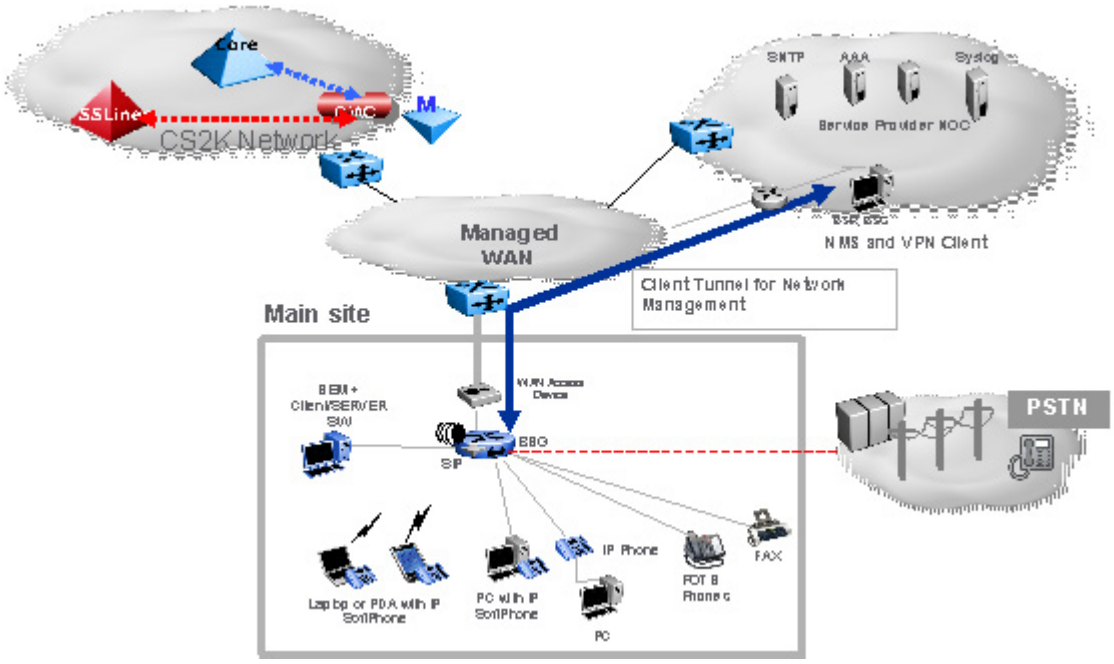
The SIP SBC monitors the approachability of the configured SIP server using SIP OPTIONS messages. When the configured SIP server is not reachable, the BSG8ew transitions to Backup mode. In the Backup mode, new call attempts will succeed as long as the calls are reachable to local endpoint or to the PSTN over FXO port.

Network management

Remote management of the BSG8ew is supported through a secure management protocol such as HTTPS, SNMPv3, and SSH. Use of unsecured protocols such as HTTP, Telnet and SNMPv1/v2c to manage BSG8ew remotely is not recommended, especially if the management traffic traverses an un-trusted domain.

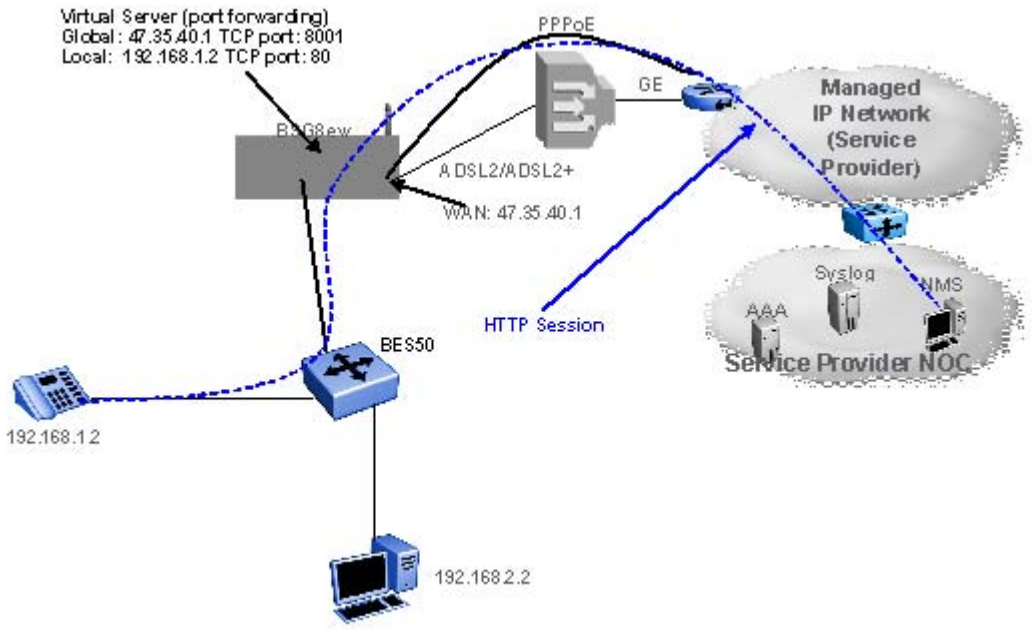
The remote management of solution components requires management connections to be terminated on the component being managed. For this to happen IP connectivity needs to be established between the management device and the device to b managed. It is not a problem in case of BSG8ew since it is directly visible to the management application as being directly connected to the public network. It becomes however more complicated for solution components other then BSG8ew. These components are located on the customer private network and they are normally not visible to the management application by their private IP addresses. They can be made visible to the application by setting up IP VPN between the management application and the BSG8ew. For example, IPSec client tunnel. In this case, the management application can communicate with the devices by their private addresses and the BSG8ew will transparently to the management protocol route IP packets carrying management traffic directly to the device. If the customer devices are dynamically assigned IP addresses from the DHCP server the address assigned to the device is not pre-determined. To uniquely identify managed device it is required that the MAC address of the device is associated with the IP address defined in the DHCP address pool.

Figure 26 IP VPN base remote management



In case when the IPSec tunnel option is not feasible a port forwarding capability of the BSG8ew can be employed to forward management traffic to the respective device based on the port number associated with this device. The management application would initiate the connection to the public address of the BSG8ew WAN interface but with the destination port that corresponds to the device to be managed. In this method the management application identifies device by port number. Example of such a configuration is presented in Figure 27 Port forwarding based remote management (page 60). The NMS application opens an http session using global BSG8ew IP address 47.135.40.1 and TCP port 8001. The virtual server on the BSG8ew forwards the http traffic to IP phone 192.168.1.2 and port 80 (well known HTTP server port).

Figure 27 Port forwarding based remote management



When deployed, the BSG8ew can be managed using either its web interface or Command Line Interface (CLI). Both interfaces can be accessed securely using HTTPS and SSH respectively. The BSG8ew can also be managed using SNMP v1/v2c/v3. After the VPN tunnel is established, the service provider can manage on site network elements using Business Element Manager (BEM) to discover nodes, and unsecured protocols such as HTTP.

Software Upgrades and Backup and Restore

BSG8ew

The software upgrade of BSG8ew can be done by downloading required software version through one of:

- FTP
- TFTP
- HTTP

Once the firmware and software packages are downloaded and stored in the flash memory the system reboots and loads a new image.

The software upgrade does not impact configuration of the BSG8ew.

The detailed Software Upgrade procedure is provided in the BSG8ew Administrator Guide.

The TFTP client can also be used to upload the saved configuration file of the BSG8ew to a TFTP server. The configuration file can then later be downloaded to the BSG8ew and activated.

LG 6000

The LG phone can download the software from one of the following servers:

- TFTP
- HTTP
- HTTPS

Once the software is downloaded the phone reboots to activate it. The detailed description of software upgrade procedure is provided in *IP Phone 6804 Installer Guide*.

Business Ethernet Switch

The Business Ethernet Switch (BES) firmware can be upgraded by simply downloading the required firmware version from a TFTP server and resetting the switch to activate it.

The configuration file can be saved on the TFTP server and then downloaded and restored on the BES50.

The detailed description of the firmware upgrade and backup and restore procedure is provided in *Using the Nortel BES 50 Guide*.

Voice calls

In the Hosted Solution the BSG8ew has a role of the intermediate agent between the SIP endpoints and the SIP Call Server located at the Hosted Solution Center. The messages that BSG8ew receives from the SIP endpoints are forwarded to the SIP call servers and the responses are forwarded back to the SIP endpoints. This is also true for the calls between the local SIP endpoints.

To support seamless communication with the SIP Call servers and between SIP endpoints themselves BSG8ew implements the following components:

- SIP proxy and registrar
- SIP ALG
- Call Admission Control
- SIP gateway for support of FXS and FXO interfaces
- WAN link monitor

SIP proxy and registrar

SIP proxy and registrar handle SIP control messages form the SIP phones connected to the private LAN segments. The SIP phones should be provisioned with the BSG8ew IP interface that they are connected to as the address of the SIP call server.

Attention: SIP proxy and registrar are always reachable through VLAN 1 interface IP address: 192.168.1.1. The SIP clients must always be provisioned with 192.168.1.1 as IP address of the SIP proxy even if they are members of subnets other VLANs (subnets other then 192.168.1.0/24).

SIP ALG

The SIP Application Layer Gateway (ALG) module, manipulates the private IP addresses in outgoing SIP messages to public IP addresses to accommodate NAT. It creates necessary mappings within the NAT module for signaling and media flows and also opens pinholes in the firewall. On the BSG8ew, the SIP ALG is automatically enabled when the NAT functionality is enabled on the WAN interface.

Call Admission Control

The Call Admission Control function ensures that there is adequate WAN bandwidth available for incoming and outgoing SIP traffic flow before the actual call is setup. The Call Admission Control module tracks the number of calls established through the WAN link and does not allow it to exceed the configured maximum value. The number of maximum calls that the CAC will allow depends on the bandwidths needs per call and that depends on the type of codec used. Example of the bandwidth requirements for different types of codec is presented in Table 13 Examples of VoIP bandwidth requirement over Ethernet based IP. The number of calls should be calculated based on the available bandwidth on the WAN link. In case of DSL consideration should be given to the fact that uplink and downlink bandwidth are not necessarily equal.

Table 13 Examples of VoIP bandwidth requirement over Ethernet based IP

Codec	Voice Payload	IP Packects per Second	IP byte Required for one Second of Voice4	Effective Bandwidth for IP Layer	Ethernet type Required for one Second of Voice5	Effective Bandwidth at Ethernet Layer
G.711	5ms = 40 bytes	200	16,000	124Kbps	18,800	150.4Kbps
G.711	10ms = 80 bytes	100	12,000	96Kbps	13,400	107.2Kbps
G.711	20ms = 160 bytes	50	10,000	80Kbps	10,700	85.6Kbps
G.729	10ms = 10 bytes	100	5,000	40Kbps	6,400	51.2Kbps
G.729	20ms = 20 bytes	50	3,000	24Kbps	3,700	29.6Kbps
G.729	40ms = 40 bytes	25	2,000	16Kbps	2,350	18.8Kbps

Call server failover

The WAN link monitoring function uses options SIP messages to monitor status of the SIP server in the Hosted Solution Center. The WAN link monitoring module also receives notifications from the WAN interfaces whenever WAN links go down or come up. This functionality allows the BSG8ew to operate in two modes:

- **Normal mode** – In this mode, the service provided managed CS2K is reachable and all calls are router via the CS2K.
- **Backup mode** – The SIP SBC monitors the approachability of the configured SIP server using SIP OPTIONS messages. When the configured SIP server is determined to offline, the BSg8ew transitions to Backup mode. In the Backup mode, new call attempts will succeed as long as the calls are reachable to local endpoint or to the PSTN over FXO port.

In addition there are two FXS and one FXO interfaces for access to the TDM network. In a Normal mode of operation the FXS are considered to be SIP endpoints. The calls from the analog or digital phones connected to the FXS interface are handled as calls from any other SIP endpoint.

Normal mode is the operational mode of the BSG8ew in which connectivity to the central SIP server is alive and routing of calls is handled by the central SIP server. Backup mode is mode of operation of BSG8ew in which connectivity to central SIP server is down and routing of calls at the site is handled by the BSG8ew.

Analog telephony and FAX

The BSG8ew has two FXS interfaces that can be used to connect analog phones and one FXO interface to connect BSG8ew to the Central Office in the PSTN network. The analog phone once connected. The service supported are presented in the following table.

Table 9 Analog telephone and FAX interworking

	BSG8eb
POTS+ Capability	1) Loop Start Signaling 2) DTMF Signaling 3) Caller ID 4) CLASS Message Waiting 5) Hook Flash
911 Access	911 routing as per Dial Plan.

In network failover mode, client Interconnection shall be limited to POTS capability. In power failover mode, a relay connection between FXS and FXO shall enable basic POTS service.

Calls connected via FXO during power or network outage shall be retained following restoration of power and network. Calls connected via FXO prior to network or power outage shall be retained following failure of power or network.

Routing of all 911 calls through FXO shall be a configurable option.

Emergency voice calls

The emergency voice calls can be routed to service provider SIP call server or they can be routed directly to the PSTN network through the BSG8ew FXO interface. How the calls are routed is controlled by the dial plan. For example, the dial plan can be configured to always send 911 calls to the FXO interface.

Another feature supported on the BSG8ew is the ability to distinguish between the emergency and non emergency calls. This feature allows handling of the emergency calls with priority over the non emergency calls. For example if there is a non emergency call already present on the FXO interface and emergency call is routed to that interface, the non emergency calls is terminated.

The emergency calls should meet the following requirements:

- Will stay up even if the power to the box is lost
- Can be established even if the power is down
- For that reason it is recommended that the emergency calls are routed to the PSTN network by means of the FXO interface

Dial plan

By default the dialing plan routes all the calls to the provisioned SIP communication server. The dialing plan can however be provisioned to route calls based on the digits dialed.

There can be two dialing plans configured on the BSG8ew, one of them is required for normal mode of operation and second one is used when the BSG8ew falls into Backup mode of operation. Only one of the dialing plans can be active at a time.

Normal dialing Plan should be setup to route the calls to the communication server in the Hosted solution Center. The Backup dialing Plan should be provisioned to route the external calls to the PSTN network through the BSG8ew FXO interface.

Data services

Various sections of this document have described data services that are important from the solution perspective. Some of the services available were not described because they were not relevant to the solution. They may however be useful for certain customer configurations, hence the full set of available data services is provided. This section is included here for the sake of completeness and as a summary of the BSG8ew capabilities with respect to the data services.

Host network considerations

WAN QoS strategy

The Nortel Networks has defined Nortel Service Classes that can be used as guidelines for implementation of end-to-end QoS. If the NNSC are used for QoS implementation in the access network, it is recommended that the core network also follows NNSC for its QoS implementation to ensure consistent end-to-end QoS support. The Nortel Service Classes guidelines are presented in section End-to-end Quality of Service (page 39) of this document.

There is no QoS to be applied on the DLS or cable link. There is no such a need since the BSG8ew applies QoS on its WAN interface in the egress direction. The next node that will need to apply QoS is the node that aggregates traffic from multiple DSL or cable access links, for example a service provider DSLAM.

The diffServ code points of the packets need to be honored by the service provider edge router (BRAS) to make sure that the packets receive required end to end QoS treatment.

Interoperability requirements and summary

Voice services

The solution components that need to be verified for interoperability:

- LG 6800 < - > CS2000 SIP Call Server
- Nortel Eybeam Client SMC 3456 < - > CS2000 SIP Call Server
- LG 6800 < - > Nortel Eybeam Client SMC 3456
- MCS Client < - > LG 6800
- MCS Client < - > Nortel Eybeam Client SMC 3456

Data services

The following data services require interoperability testing:

- BSG8ew SIP Proxy < - > CS2000 SIP Call Server
- SafeNet IPSec Client < - > BSG8ew IPSec Client Termination
- IPSec Client Termination < - > NAT Traversal
- IPSec Branch-to-Branch tunnel< -> NAT Traversal
- MCS Client

Performance and capacity summary

This section provides information on the capacity of the BSG8ew with respect to the services that it supports.

Table 15 – BSG8ew capacity numbers

Attribute	Maximum limit
Number of ports for RSTP functioning	8
Number of MSTP instances	4
Number of VLANs	64
Number of learnt MAC addresses	4096
Number of ports for 802.1x authentication	16
Number of IP interfaces	128
Number of static routes	16
Number of routes in RIP routing table	256
Number of routes in OSPF routing table	512
Number of simultaneous SIP calls	50
Number of OSPF interfaces	16
Number of OSPF areas	16
Number of OSPF adjacencies	16
Number of IPSec tunnels	64
Firewall - number of policies	1024
Firewall - number of flows	5000
NAT - number of policies	16
NAT - number of flows	1024
WiFi access - number of clients	16
QoS - number of egress CoS queues per port	8
ACL - number of filters	100
ACL - number of rules/policies	100
Number of simultaneous OSPF adjacencies	50
Number of static DHCP mappings in DHCP server (mapping of IP address to MAC address)	16

Reference topologies

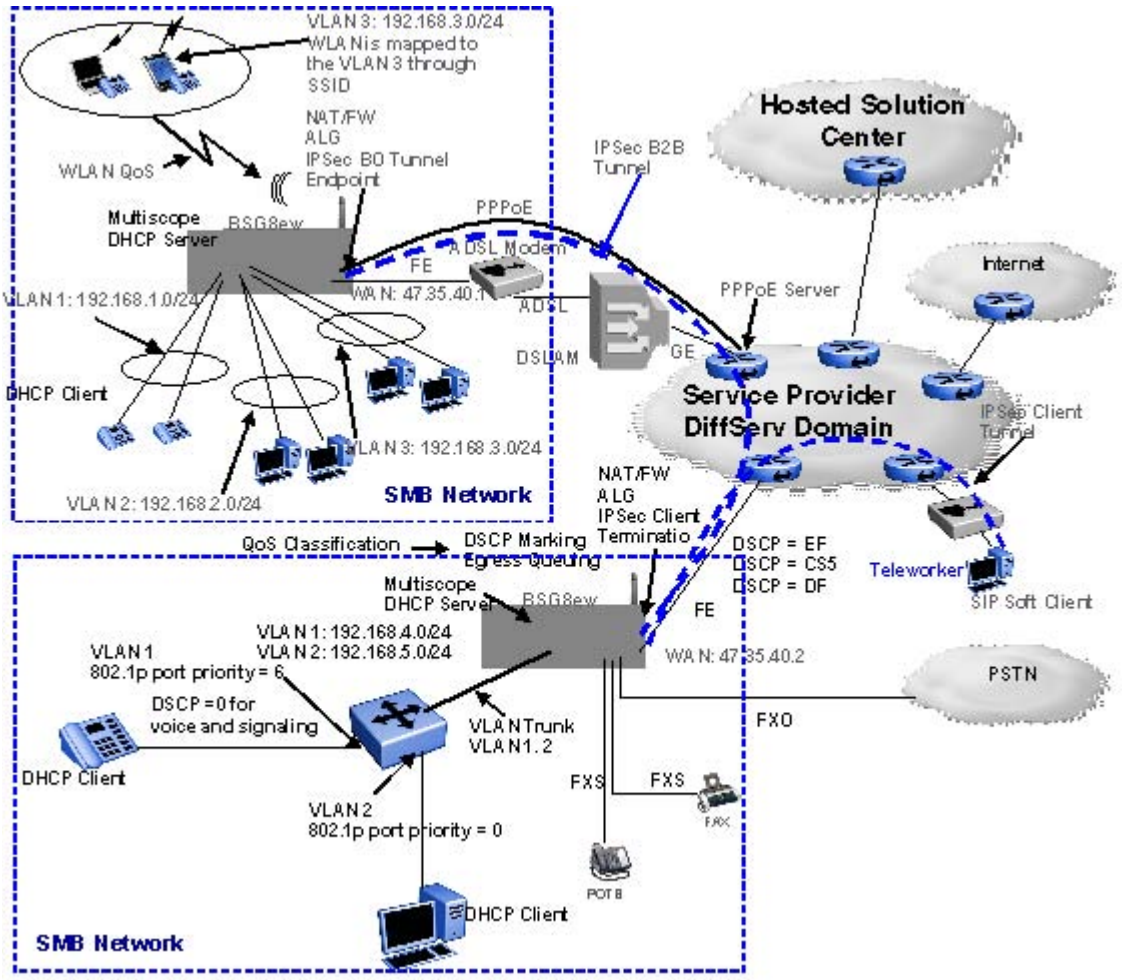
Products are designed with these reference topologies and configurations in mind, and validated with respect to these reference topologies prior to release. As a first step, it is recommended that the channels replicate these reference topologies in their lab and use them as a reference point. The Small and Medium (SMB) market place is diverse, and it is hoped that the versatility of these products enable solutions not envisaged by their designers. The end customers unique requirements are addressed by building a modified configuration, subject to engineering recommendations and constraints highlighted in the General considerations (page 33) section of this document.

This initial release of the BSG8ew is targeted at a service provider model where the equipment is owned and managed by a service provider. It is assumed that the BSG8ew and other supporting SMB equipment (switches and access points) are configured by the service provider prior to being shipped to the SMB.

It is expected that a service provider will be deploying many thousands of BSG8ews. To facilitate user account administration, the service provider may choose to manage a centralized AAA server (TACACS/RADIUS server) against which users logging into the BSG8ew will be authenticated. Similarly, the service provider manages centralized SNTP for time synchronization, Syslog for receiving Syslog messages from BSG8ews and an NMS for receiving SNMP traps from the BSG8ew.

The reference topologies are the subsets of the SMB – Hosted Solution Architecture described in Figure 28 – SMB – Hosted Solution Architecture (page 70). The purpose of the SMB – Hosted Solution Architecture is to identify the areas of interest that need to be considered when designing the Customer Topology. The various components of the SMB – Hosted Solution Architecture can be extracted and put together to create the customer specific solution.

Figure 28 – SMB – Hosted Solution Architecture



Topology 1 — Data and SIP voice services

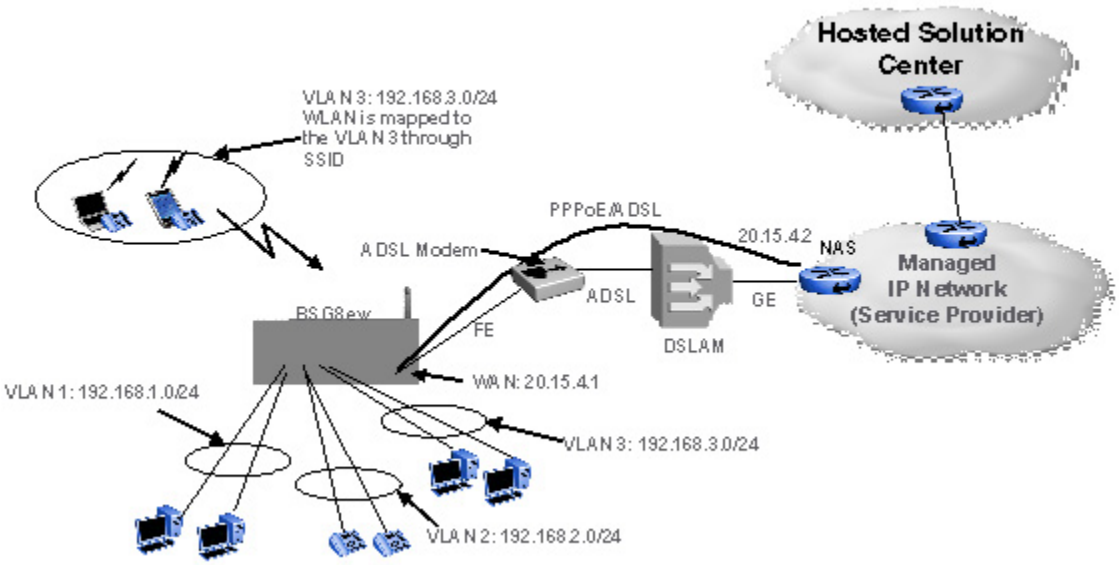
Figure 29 – Reference topology 1 (page 71) illustrates how the BSG8ew can be used to realize reference topology 1 using an ADSL as the WAN access device. This topology can also be realized with either a cable modem or an Ethernet drop from a Provider Edge Router (PER) as the WAN access device. If ADSL is used, the BSG8ew uses PPPoE to authenticate and obtain IP related parameters from the service provider in contrasts to using DHCP to obtain parameters from the service provider.

Attention: IP address assigned to the WAN interface of the BSG in scenario must be routable with the service provider WAN, i.e, NAT must be disabled on the PER or if enabled, the PER must have a SIP ALG.

In a reference topology 1, the BSG8ew is configured with the following information:

- PPPoE client enabled on the WAN interface (The IP address is assigned to the client during IPCP exchange)
- Three VLANs with the following VLAN interfaces:
  - — Ethernet Port 0 and 1: VLAN 1: 192.168.1.0/24
  - — Ethernet Port 2 and 4: VLAN 2: 192.168.2.0/24
  - — Ethernet Port 5 and 6: VLAN 3: 192.168.3.0/24
- L2 QoS:
  - — VLAN 1 port: priority 6 (Voice VLAN)
  - — VLAN 2 port: priority 3 (Data VLAN)
  - — VLAN 3 port: priority 0 (Guest VLAN)
- Enabled DHCP Server with three address scopes: 192.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24
- Configure SIP Proxy with the IP address of the Hosted Solution SIP server
- Dial plans for normal and backup mode

Figure 29 – Reference topology 1



Configuration steps

This section describes the procedures for configuring BSG8ew to realize SMB reference topology 1.

Assumptions

- This is the initial configuration of the BSG8ew.

- CS2K network is configured and is ready for use, i.e., user accounts for SIP users of the BSG8ew are configured on the CS2K.
- The NOC has the following functions installed and configured:
  - An SNTP server within the service provider NOC is configured with the date and time.
  - A TACACS server is configured with the account details of users that will be managing the BSG8ew.
  - A Syslog server is available for is receiving logs from the BSG8ew.
  - TFTP server with the firmware and/or configuration files for SIP sets that will be connected this BSG8ew.
  - A Network Management Station (NMS) that supports SNMPv3 has the BSG8ew MIBs installed.
  - Configure the NMS with credentials and security settings required secure SNMPv3 messages between the BSG8ew and NMS.
- NAS is configured with the credentials of the BSG8ew to allow PPPoE client termination.

Configuration procedures

The topology 1 configuration can be divided into following blocks:

- User account management
- VLAN and interface configuration.
- Multi-scope DHCP server configuration
- SIP configuration
- Firewall configuration
- QoS configuration
- SNMP agent configuration
- Syslog configuration
- WLAN configuration

User account management configuration

- Using your preferred management interface, login into BSG8ew with username and password as nnadmin and PlsChgme! respectively.
- Create a new administrator account that matches the administrator account created on the TACACS+ server. At minimum, change the default password of the default nnadmin account.
- Configure the BSG8ew to authenticate remote logins using TACACS and local data base as last resort in the event the TACACS server is unreachable.

WAN configuration

Access to the service provider managed WAN can be provided via one of the following three options:

ADSL access

- The BSG8ew connects to the service provider infrastructure through an external DSL modem. It is assumed that
  - The service provider will configure the ADSL modem before deploying it at the customer premise.
  - The DSL modem acts a bridging device to relay PPPoE frames originated from the BSG8ew onto the DSL link.
- If means of access is ADSL, enable PPPoE on the WAN interface of the BSG8ew and configure the username, password for authentication.
- Configure the PPP interface to dynamically acquire IP address and other related parameters from the service provider. Otherwise, configure the PPP interface with IP address, netmask, DNS server and default router if using static addressing.

Cable modem access

- The BSG8ew connects to the service provider infrastructure through an external cable modem. It is assumed that
  - The service provider will configure the cable modem before deploying it to the customer.
  - The cable modem acts a bridging device to relay Ethernet frames originated from the BSGew.
- In this case, configure the WAN interface to dynamically acquire IP address and other related parameters from the service provider. Otherwise, configure the interface with IP address, netmask, DNS server and default router if using static addressing.

Ethernet access

- The BSG8ew connects directly to the service provider Ethernet based network infrastructure.
- In this case, configure the WAN interface to dynamically acquire IP address and other related parameters from the service provider. Otherwise, configure the interface with IP address, netmask, DNS server and default router if using static addressing.

VLAN configuration

- Create three VLANs named Data, Voice and Guest respectively.
- Configure Ports 1 and 2 as untagged member of the Data VLAN
- Configure Port 3 and 4 as an untagged member of the Voice VLAN
- Configure Port 5 and 6 as untagged member of the Guest VLAN.
- Create three virtual interfaces corresponding to the configured VLANs:
  - The interface associated with the Data VLAN (IP@192.168.1.1/24)
  - The interface associated with the Voice VLAN (IP@192.168.2.1/24)
  - The interface associated with the Guest VLAN (IP@192.168.3.1/24)

Multi-scope DHCP server configuration

- Create DHCP Server Pool 1 for serving DHCP clients on the Data VLAN
- Create DHCP Server Pool 2 for serving DHCP clients on the Voice VLAN

  - — Configure the TFTP server name option (option 66) as the IP address TFTP server IP address in the NOC.
  - — Configure time server option (Option 4) with the IP address of the service provider SNTP server.
  - — Configure the time offset option (Option 2) with a value that reflects your region offset from UTC.
- Create DHCP server pool 3 for serving DHCP clients on the Guest VLAN

SIP configuration

- Configure the SIP proxy with the domain name of the managed service
- Configure the proxy with the IP address of the CS2K as well as the following parameters:
  - — SIP transport protocol as UDP that will be used for polling the CS2K
  - — SIP port number as 5060
  - — Poll interval as 600 seconds. BSG8ew will send a SIP ping every poll interval to determine the health of the CS2K
  - — Poll retries set to 3. The CS2K will be declared as down after 3 successive failed retries.
- Configure the SIP registrar on BSG8ew to dynamically learn and add user names of SIP client to its local database.
  - — Enable both FXS 1 and FXS 2 on the BSG8ew.
  - — Configure FXS 1 with the display name, number and password required for authentication against the CS2K.
  - — Configure FXS 2 with the display name, number and password required for authentication against the CS2K.
  - — Configure the BSG8ew with the maximum number of simultaneous calls that should be allowed across the WAN. See the QoS configuration section for details of how to calculate this number.
  - — Create a dial plan for normal mode operation and download it to the BSG8ew using FTP. This is the dial plan used when the service provider managed CS2K is online and reachable from the BSG8ew.
  - — Create a backup dial plan and download it to the BSG8ew using FTP. This is the dial plan that will be used when the service provider managed CS2K is not reachable from the BSG8ew e.g, when the WAN link is down.
  - — Reload all the dial plans.

Firewall configuration

- Create the following firewall rules to allow the service provider to manage the BSG8ew from the NOC.
- Permit SSH access.
- Permit secure web access (https) from within the service provider NOC.
- Permit SNMP from service provider NMS.
- Permit TFTP/FTP traffic from SIP sets on the LAN to only the TFTP/FTP server in the NOC.

- Configure both the data and Voice VLANs as trusted interfaces and configure the Guest VLAN as untrusted interface.
- Permit WAN access to the guest VLAN.
- Deny hosts on the guest VLAN from reaching the data and voice VLANs.

Virtual server configuration

- Configure a virtual server for SSH on the WAN interface. This will allow the network operator to manage the BSG8ew using SSH from the NOC.
- Configure a virtual server for HTTPS on the WAN interface to allow the BSG8ew to be managed securely using the Web UI from the NOC.
- To allow management using SNMP from the NOC, a virtual server must be configured on the WAN interface.

QoS configuration

- Enable QoS on the BSG8ew.
- Determine your WAN bandwidth from your service provider and determine how much of the available bandwidth must be reserved for VoIP traffic. Using this value, calculate the maximum number of simultaneous call can be supported by dividing the bandwidth reserved for voice by the bandwidth required for each call. See Table 16 Examples of VoIP bandwidth requirement over Ethernet based IP (page 76) for bandwidth requirement for different CODECs. Based on the calculations configure maximum number of calls.
- Create a layer 3 classification rule for VoIP media and SIP signaling. VLAN Id or subnet address of the voice VLAN can be used as the input to the classifier.
- Create a layer 3 classification rule for data VLAN using the subnet address of the data VLAN to classify the flow.
- Create a layer 3 classification for the guest VLAN using the subnet address of the guest VLAN to classify the flow.
- Configure DSCP value to be set in the packets matching the classifier. Configure priority to be applied to the packet matching the classifier. Make sure that the Voice traffic is sent to Strict Priority queue. Queue priority vs queue numbering follows the following rule:
  Egress Queue = 7 - 802.1p priority (see Appendix for details on QoS support on BSG8ew). For example, if the priority is 6 then, the corresponding queue number is 1. That means that if the classifier sets the priority for the incoming packet to 6 the packet is sent to queue # 1.
- Configure strict priority scheduler for the voice egress queue (in our example it is queue 1) and WRR for remaining queues.
- Assign weights to each of the traffic class queues on the WAN port.
- Create one Policer rule for voice using the trTCM policing algorithm according to values shown below (assuming G.711 is used as CODEC):

Table 16 Examples of VoIP bandwidth requirement over Ethernet based IP (page 76) shows examples of the bandwidth required for G.711 and G.729 at various voice sample sizes.

Table 16 Examples of VoIP bandwidth requirement over Ethernet based IP

Codec	Voice payload	IP packets per second	IP byte required for one second of voice	Effective bandwidth at IP layer	Ethernet byte required for one second of voice	Effective bandwidth at Ethernet layer
G.711	5ms = 40 bytes	200	16,000	128Kbps	18,800	150.4Kbps
G.711	10ms = 80 bytes	100	12,000	96Kbps	13,400	107.2Kbps
G.711	20ms = 160 bytes	50	10,000	80Kbps	10,700	85.6Kbps
G.729	10ms = 10 bytes	100	5,000	40Kbps	6,400	51.2Kbps
G.729	20ms = 20 bytes	50	3,000	24Kbps	3,700	29.6Kbps
G.729	40ms = 40 bytes	25	2,000	12Kbps	2,350	18.8Kbps

Attention: Assume no IP header options.

Total size of RTP, UDAP and IP header is 40 bytes.

Exclude Ethernet preamble and FCS, and no 802.1p/q tag in Ethernet frames on WLAN uplink interface. Ethernet overhead is 12 bytes.

- Map the Policer ID for voice to the classification rule for voice traffic configure in the Step Create a layer 3 classification rule for VoIP media and SIP signaling. VLAN Id or subnet address of the voice VLAN can be used as the input to the classifier.
- Create a second Policer rule for data, again using the trTCM algorithm with values for PIR, CIR, PBS and CBS set according to the following:
  - DataPIR (bps) = Available WAN bandwidth
  - DataCIR (bps) = Available WAN bandwidth - VoicePIR (bps)
  - PBS = 1500bytes
  - CBS = 1500bytes

The above configuration allows data to burst up to the maximum available bandwidth when there is no voice traffic but will be discarded in favor of VoIP traffic when there is competition between VoIP and data.

- Map the Policer ID for data to the classification rule for data traffic configured in the classification rule for data step in QoS configuration (page 75).
- Similarly, configure a Policer ID for traffic from the Guest VLAN by setting the following trTCM parameters as follows:
  - DataPIR (bps) = Available WAN bandwidth
  - DataCIR (bps) = Available WAN bandwidth - VoicePIR (bps)

  - PBS = 1500bytes
  - CBS = 1500bytes
- Map the Policer ID created for the guest VLAN configured in the classification rule for guest step in QoS configuration (page 75).

SNMP configuration

- Enable SNMPv3 and disable the other SNMP versions.
- Configure the system location, system contact and system description attributes.
- Configure the SNMPv3 agent with a username and password on whose behalf SNMP messages are exchanged with the NMS. This user account should have been created on the NMS.
- Configure the SNMPv3 agent with security setting to use both authentication and privacy to protect SNMP messaging.
- Specify the IP address of the NMS as the TRAP receiver.
- Configure the SNMP agent to send TRAPs when the following events occur:
  - Link up
  - Link down
  - Cold start

Syslog configuration

- Enable the Syslog client on the BSG8ew.
- Configure the BSG8ew with the IP address of Syslog server.
- Specify the severity levels of logs for which Syslogs messages will be generated and sent to the server.

WLAN configuration

- Select the country code matching the country in which the BSG8ew is installed.
- Enable the WLAN AP on the BSG8ew.
- Enable WMM for service differentiation over the air, and tag uplink Ethernet frames with the 802.1p values in accordance with Wi-Fi Alliance WMM specification:

Table 17 – WMM 802.1D priority to access class mappings

Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation
lowest	1	BK	AC_BK	Background
	2	-		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
highest	7	NC		

- Create 3 SSIDs.
  - SSID 1 (Data SSID)
  - SSID 2 (Voice SSID)
  - SSID 3 (Guest SSID)
- Configure the BSG8ew for SSID 1 (Data SSID) according to the following:
  - Enable WPA1-PSK or WPA2-PSK
  - Disable broadcast SSID
  - Map this SSID to the VLAN ID for the Data VLAN
- Configure the BSG8ew for SSID 2 (Voice SSID) according to the following:
  - Enable WPA1-PSK or WPA2-PSK
  - Disable broadcast SSID
  - Map this SSID to the VLAN ID for the Voice VLAN
- Configure the BSG8ew for SSID 3 (Guest SSID) according to the following:
  - Enable WPA1-PSK or WPA2-PSK but ensure that the pre-shared key for this guest SSID is different for that configured for the data and voice SSIDs
  - Disable broadcast SSID on this SSID.
  - Map the guest SSID to the guest VLAN ID created earlier on the BSG8ew.
- Enable all three SSIDs

Save configuration changes

- Save configuration changes to flash
- Back-up the start-up configuration file to a remote machine using FTP.

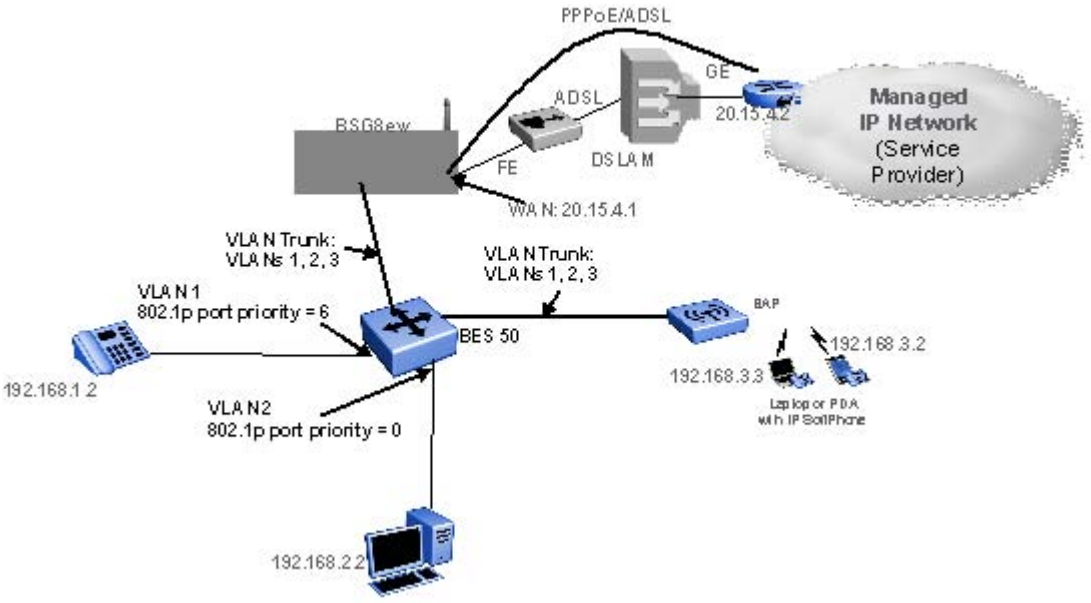
Connecting the dpevices

- Plug PCs into LAN ports of the BSG8ew that are member of the data VLAN
- Connect the SIP phones into LAN ports of the BSG8ew that are members of the voice VLAN
- Reserve the ports that are members of the guest VLAN for visitors of the SMB.

Topology 2 - Data and SIP Voice with port expansion and mobility

The topology 2 expands topology 1 by adding the Ethernet switch to increase the number of available LAN ports. The topology 2 is suitable for larger SMB sites with the number of devices that exceed the number of Ethernet ports available on BSG8ew which is eight.

Figure 30 – Reference topology 2



The BES switch is connected to the BSG8ew Gigabit Ethernet port 8. The L2 topology is the same as for reference topology 1. There are three VLANs defined:

- VLAN 1: is used for PCs
- VLAN 2: connects LG Phone
- VLAN 3: is a guest VLAN

In a reference topology 2, the BSG8ew is pre-configured with the following information:

- Default gateway address: 20.15.4.2 (provided by the service provider)
- Three VLANs with the following VLAN interfaces:
  - Ethernet port 1 and 2: VLAN 1: 192.168.1.0/24
  - Ethernet port 3 and 4: VLAN 2: 192.168.2.0/24
  - Ethernet port 5 and 6: VLAN 3: 192.168.3.0/24
  - Ethernet port 7 (VLAN Trunk): VLAN 1, VLAN 2, VLAN 3

- QoS—The QoS mechanisms are applied to the packets both on BSG8ew and on the BES. The packets are prioritized in both WAN to LAN and LAN to WAN direction. In WAN to LAN direction the packets that are received from the WAN link are classified based on their DSCP value and are marked with the 802.1p bit value as required. In the WAN to LAN direction the packets are prioritized as per default settings for DSCP to 802.1p mapping presented in . For example the voice packet marked with DSCP = EF received on the WAN interface will be marked with 802.1p = 6 before it is sent out the VLAN trunk port 7. On the other hand, the data packet marked with DSCP = DF will be marked with the 802.1p = 0 before sending it out the VLAN trunk.

In LAN to WAN direction, the packets can be prioritized based on the port priority of the port that the sender is connected to. So the BES ports that IP phones are connected to, VLAN 1, are assigned port priority of 6. The BES ports that the PCs are connected to, VLAN 1, are assigned the port priority of 3. The packets received from BAP 120 are assigned a default 802.1p bit of 0 at the BAP end.

- Enabled DHCP Server with three address scopes: 192.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24
- IP address of the communication server
- Dial plans for normal and backup mode

Configuration steps

Reference topology 2 includes two additional Nortel SMB devices namely the BES Ethernet switch in addition to the BSG8ew. The configuration steps for the BSG8ew are similar to procedure outlined for reference topology 1.

Topology 2 requires configuring BES50 port 7 as a trunk port and a member of VLANs 1, 2 and 3.

The configuration steps for the BES Ethernet switch and the BAP120 wireless AP are described in the following sections.

BES50 configuration

Configuration tasks at a glance

- User management configuration
- Network management related OAM configuration
- VLAN configuration
- Quality of Service configuration
- Authentication – the devices are authenticated locally at the BES50 using 802.1x.

Step-by-step configurations

User management configuration

1 Log onto the BES50 using the default username and password.

2 Change the password of the default username.

Network management related OAM configuration

1 Configure the BES50 to use the SNTP server located in the service provider network.

2 Configure the BES50 to use the Syslog server located in the service provider network.

Configure SNMP agent

1 Modify the system location, system contact and system description attributes if needed.

2 Modify the read community string to match the one used by the service provider, and the address of the Network Management Station (NMS).

3 Modify the write community string to match the one used by the service provider, and the NMS address.

4 Configure the trap community string to match the one used by the service provider, and the address of the SNMP trap receiver located in the service provider network.

5 Create SNMPv3 user account to match the user credentials establish on the NMS:

- Username.
- Authentication setting including authentication algorithm and password.
- Privacy setting including encryption algorithm and password.

6 Configure SNMPv3 group to use SNMPv3 security model for message processing.

VLAN configuration

By default, all the ports of the BES50 are part of a LAN 1. Skip this step if only a single LAN is needed in the customer premises network. Configure 3 VLAN as follows:

1 Create the 3 VLAN recommended by Nortel.

2 Modify the VLAN membership of the ports to reflect the customer premises deployment.

VLAN ID	Description
1	Native VLAN, Management and Data traffic
2	Voice over IP traffic
3	Guest traffic

For BES50 with 12 ports

1 Configure Port 1 as 8021.Q trunk and as member of all the VLANs. Outgoing Ethernet frames are tagged with 802.11 tag, and incoming frames are tagged with appropriate 802.1p/q tags. This is the port connecting BES50 to BSG8ew.

2 Configure Port 2 as 8021.Q trunk and as member of all the VLANs. Outgoing Ethernet frames are tagged with 802.11 tag, and incoming frames are tagged with appropriate 802.1p/q tags. This is the port connecting BES50 to BAP120.

3 Configure Port 3 to 8 as untagged members of the Voice VLAN.

4 Configure Port 9 to 11 as untagged members of the Data VLAN.

5 Configure Port 12 as untagged members of the Guest VLAN.

For BES50 with 24 ports

1 Configure Port 1 as 8021.Q trunk and as member of all the VLANs. Outgoing Ethernet frames are tagged with 802.11 tag, and incoming frames are tagged with appropriate 802.1p/q tags. This is the port connecting BES50 to BSG8ew.

2 Configure Port 2 as 8021.Q trunk and as member of all the VLANs. Outgoing Ethernet frames are tagged with 802.11 tag, and incoming frames are tagged with appropriate 802.1p/q tags. This is the port connecting BES50 to BAP120.

3 Configure Port 3 to 12 as untagged members of the Voice VLAN.

4 Configure Port 13 to 20 as untagged members of the Data VLAN.

5 Configure Port 21 to 24 as untagged members of the Guest VLAN.

Quality of service configuration

Priority queues

BES50FE provides 4 traffic classes to prioritize network traffic: the lowest priority traffic class is 0 and the highest priority class is 3. Table 18 – BES50FE default traffic classes (page 83) lists the BES50FE default initial mappings of 802.1p values to traffic classes.

Table 18 – BES50FE default traffic classes

Traffic Class	Port Number	IEEE 802.1p Tag
0	All Ports	1, 2
1		0, 3
2		4, 5
3		6, 7

BES505E provides 8 traffic classes to prioritize network traffic: the lowest priority traffic class is 0 and the highest priority class is 7. Table 19 – BES50GE default traffic classes (page 84) lists the BES50GE default initial mappings of 802.1p values to traffic classes.

Table 19 – BES50GE default traffic classes

Traffic Class	Port Number	IEEE 802.1p Tag
0	All Ports	1
1		2
2		0
3		3
4		4
5		5
6		6
7		7

Scheduling methods

Two scheduling methods are available to determine which traffic class will be served:

Weighted Round Robin (WRR)

All classes are serviced depending on the weight assigned to the class. No starvation occurs, so that even the lowest priority class eventually receives service.

Strict

All priority packets are serviced from a class until that queue for that class is empty, and then the next lower-priority class is serviced, and so on. Starvation can occur: the traffic load for a higher-priority class can prevent lower-priority classes from being serviced.

If the customer premises has real-time traffic like VoIP through the network, strict priority queuing is recommended. Select WRR for data only network.

Packet classification

With the exception of traffic coming from BAP120, BES50 uses the ingress port to classify incoming Ethernet frames to a priority value, which in turns maps into a priority queue for service differentiation.

Ethernet frame coming from BAP120 is already tagged with the appropriate 802.1p value that maps into one of the priority queue.

Configure default port priority of BES50 as follows:

For BES50 with 12 ports

Port Number	Priority Value	Description
3 to 8	6	Voice over IP traffic
9 and 10	3	Native VLAN, Management and Data traffic
11 and 12	1	Guest traffic

For BES50 with 24 ports

Port Number	Priority Value	Description
3 to 12	6	Voice over IP traffic
13 and 10	3	Native van, Management and Data traffic
21 and 24	1	Guest traffic

BAP120 configuration

Configuration tasks at a glance

- Country code configuration
- User management configuration
- Network management related OAM configuration
- SSID configuration
- Enable WMM

Step-by-step configuration

Country code configuration

1. Log onto the BAP120 using the default username and password.
2. Select the appropriate country code (either US or Canada).
3. Reboot the access point to activate the selected country code.

User management configuration

1. Log onto the BAP120 using the default username and password.
2. Change the password of the default username.

Network management related OAM configuration

1. Configure the BES50 to use the SNTP server located in the service provider network.
2. Configure the BES50 to use the syslog server located in the service provider network.

Configure SNMP agent

1. Modify the system location, system contact and system description attributes if needed.
2. Modify the read community string to match the one used by the service provider, and the address of the Network Management Station (NMS).
3. Modify the write community string to match the one used by the service provider, and the NMS address.
4. Configure the trap community string to match the one used by the service provider, and the address of the SNMP trap receiver located in the service provider network.

SSID configuration

By default, only the 802.11b/g radio is enabled and with only one SSID created for the access point. Create and configure three SSIDs to match the VLAN configuration for BSG8ew and BES50:

Table 20 – BAP120 SSID to VLAN ID mapping

SSID	VLAN ID	Description
Data	1	Native vlan, Management and Data traffic
Voice	2	Guest traffic
Guest	3	Voice over IP traffic

1. Modify SSID 1 (Data SSID) as follows:
   - Change the SSID name to “Data”.
   - Enable WPA-PSK or WPA2-PSK.
   - Configure the pre-shared key.
   - Disable broadcast SSID
   - Map this SSID to the VLAN ID 1 for the Data VLAN.
2. Modify SSID 2 (Voice SSID) as follows:
   - Enable SSID 2.
   - Change the SSID name to “Voice”.
   - Enable WPA-PSK or WPA2-PSK.
   - Configure the pre-shared key, and ensure the pre-shared key is different from other SSID.
   - Disable broadcast SSID
   - Map this SSID to the VLAN ID 2 for the Voice VLAN.
3. Modify SSID 3 (Guest SSID) as follows:
   - Enable SSID 3.
   - Change the SSID name to “Guest”.

- Enable WPA-PSK or WPA2-PSK.
- Configure the pre-shared key, and ensure the pre-shared key is different from other SSID.
- Disable broadcast SSID.
- Map this SSID to the VLAN ID for the Guest VLAN.

Enable WMM

By default, WMM is disabled on BAP120. Enable WMM for service differentiation over the air, and tag uplink Ethernet frames with the 802.1p values in accordance with Wi-Fi Alliance WMM specification.

Table 21 – WMM 802.1D priority to access class mappings

Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation
lowest ↓ highest	1	BK	AC_BK	Background
	2	-		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
	7	NC		

Device connection

1 Connect BES50 port number 1 to port 8 of BSG8ew.

2 Connect BAP120 to BES50 port number 2.

3 Connect the LAN devices (if any) to the appropriate BES50 Ethernet LAN ports, leave LAN ports to auto-sensing.

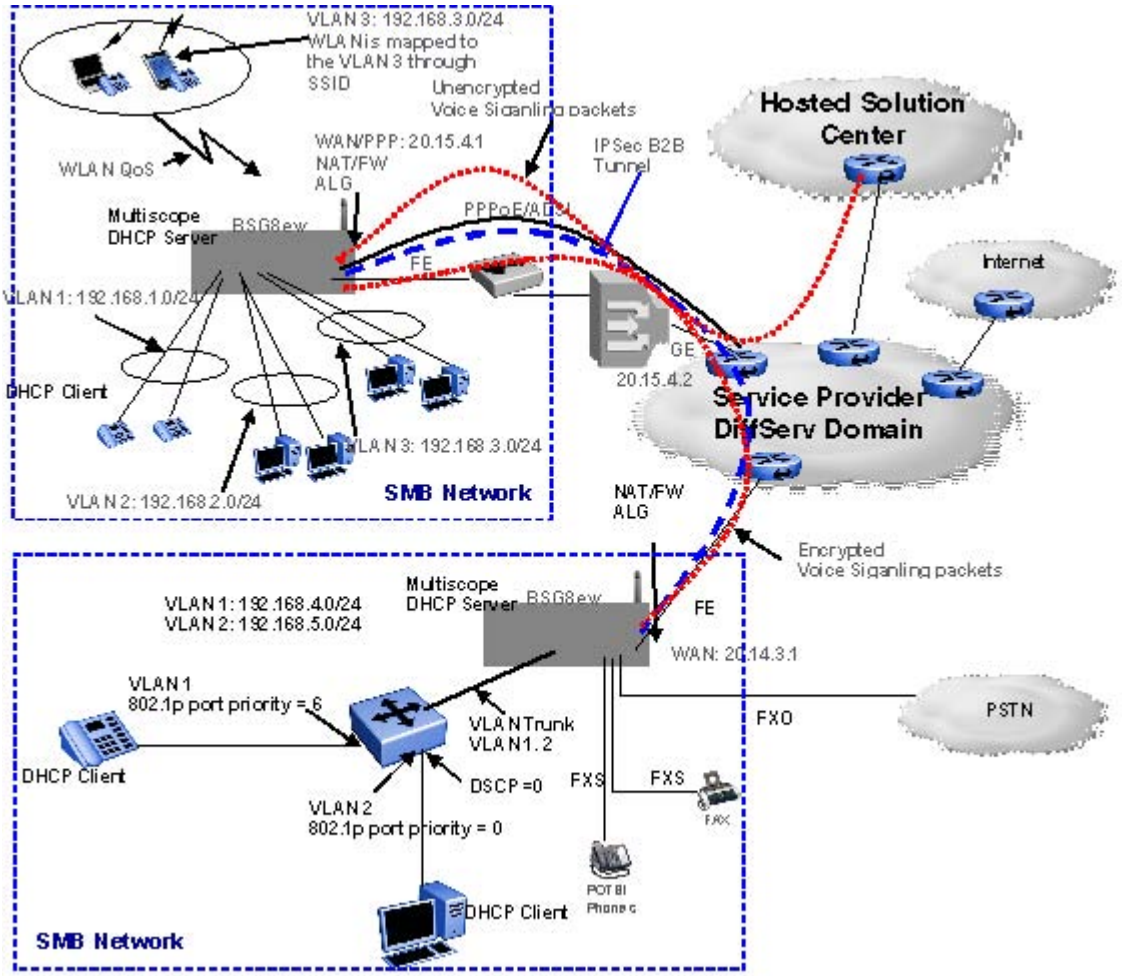
4 Connect the LAN devices (if any) to the BSG8ew Ethernet LAN port 1-3, leave LAN ports to auto-sensing.

5 Connect the WAN port to the WAN access device provided by the service provider.

Topology 3 - Data and SIP voice with IP VPN between main and branch site

The reference topology 3 illustrated in Figure 31 – Reference topology 3 (page 88) builds on topology 1 and topology 2. It is designed for customers that require secure communications between multiple sites. The Branch-to-Branch IPSec tunnel is established between two BSG8ew sites. Addition of BO tunnel does not impact other services that are present in topology like NAT/FW, DHCP, QoS and VLAN.

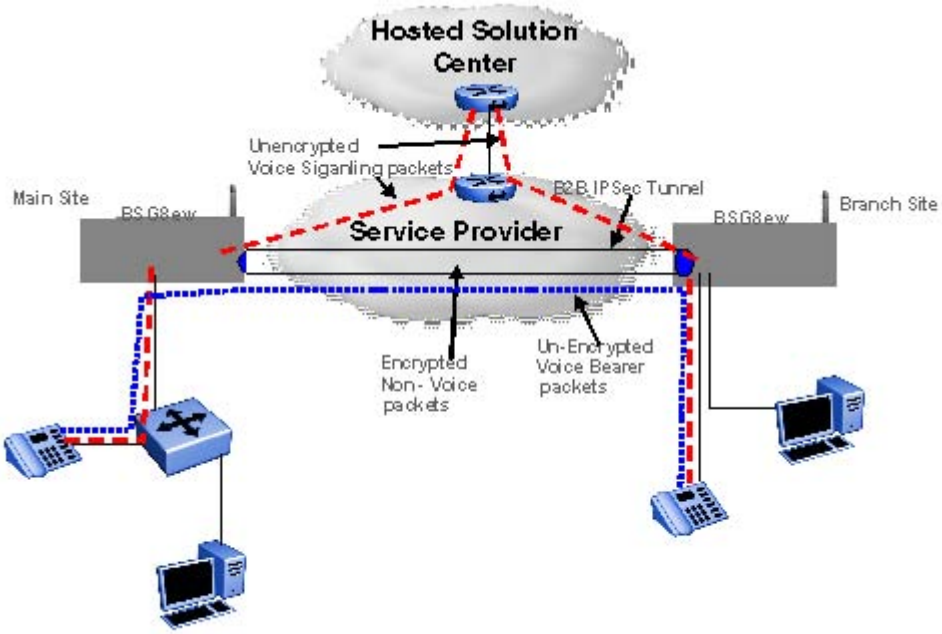
Figure 31 – Reference topology 3



There are two different ways of setting up SMB enterprise with multiple sites with respect to voice signaling path. The two options are presented in Figure 32 – Both main and branch site communicate with the call server directly (page 89) and Figure 33 – Branch site sends signaling packets to the main site BSG8ew SIP proxy (page 90).

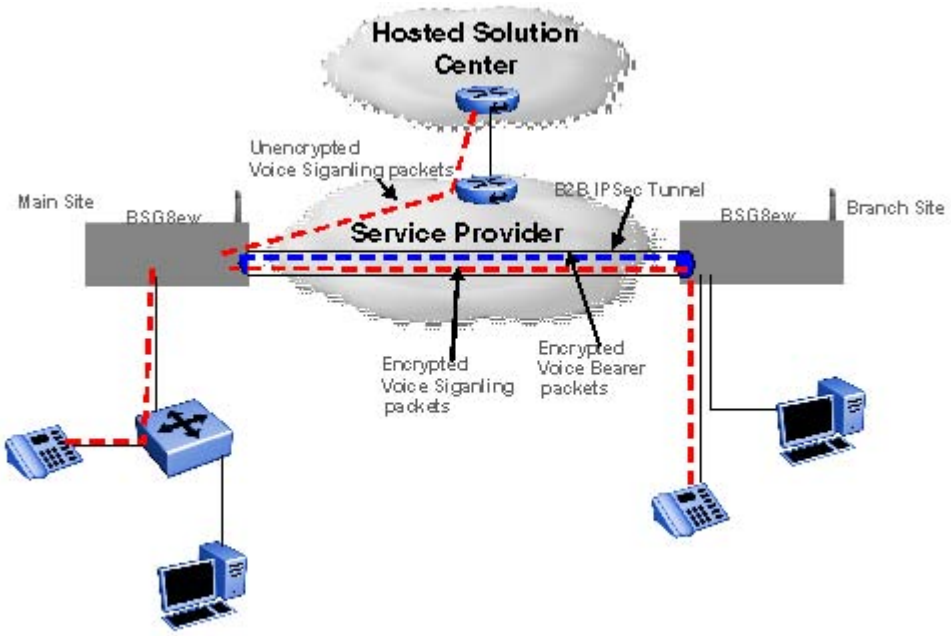
In the first option both BSG8ews send SIP signaling packets directly to the Hosted Solution SIP call server. In this case each BSG8ew is provisioned with the IP address of the Hosted Solution SIP call server. The media packets for voice calls between the two BSG8ews will not be sent through the IPSec tunnel in this configuration. Thus, this configuration is not recommended.

Figure 32 – Both main and branch site communicate with the call server directly



In the second option (Figure 33 – Branch site sends signaling packets to the main site BSG8ew SIP proxy (page 90)) the main site BSG8ew communicates directly with the hosted solution call center, but the branch site BSG8ew is provisioned with IP address of the main site BSG8ew as IP address of the SIP call server. The branch site BSG8ew does not communicated directly with the hosted solution center SIP call server but rather through the main site BSG8ew.

Figure 33 – Branch site sends signaling packets to the main site BSG8ew SIP proxy



Attention: A Branch-to-Branch tunnel configuration requires the BSG8ew PPPoE WAN interface IP address to be statically assigned. The dynamic assignment is not allowed because the IP address of the BSG8ew PPPoE WAN interface needs to be known at the time of configuring Branch-to-Branch tunnel endpoints.

Configuration steps for topology 3 are essentially the same as of topology 1 and 2 except that the BO tunnel is configured to provide the secure connectivity between two BSG8ews. Both sides are configured either for topology 1 or topology 2 and in addition IPSec BO tunnel is configured between the two BSG8ews.

To enable secure communication between the two customer sites refer the following steps.

Site-Site VPN configuration steps at main site

1. Create a Site to Site VPN policy.
2. Configure BSG8ew at HQ to use a pre-shared to authenticate the remote end of the tunnel.
3. Configure unit to use tunnel mode.
4. Provide the identity of the remote end of the tunnel.
5. Configure the HQ BSG8ew to use its WAN IP address as its identity.
6. Provide the security association parameters for IKE

7 Provide the IPSec security association parameters.

8 Define an access list that defines the traffic that will be protected by this VPN policy.

9 Configure the BSG8ew with the IKE pass phrase.

10 Bind the configured policy to the WAN interface, in this case ppp 1.

Site-Site VPN configuration steps at remote site

1 Create a Site to Site VPN policy

2 Configure BSG8ew at the remote office to use a pre-shared to authenticate the remote end of the tunnel.

3 Configure unit to use tunnel mode.

4 Provide the identity of the remote end of the tunnel.

5 Configure the remote office BSG8ew to use its WAN IP address as its identity.

6 Provide the security association parameters for IKE.

7 Provide the IPSec security association parameters.

8 Define an access list that defines the traffic that will be protected by this VPN policy.

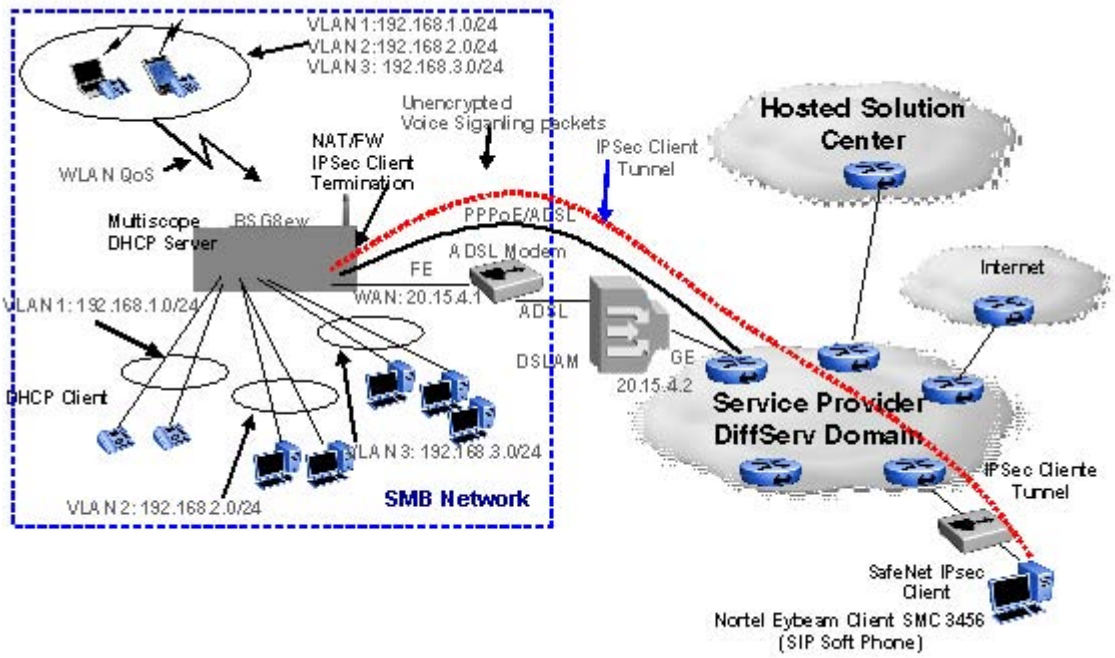
9 Configure the BSG8ew with the IKE pass phrase.

10 Bind the configured policy to the WAN interface.

Topology 4 - Data and SIP voice with IPSec client termination (teleworking)

The topology 4 also builds on topology 1 and 2. It adds IPSec client tunnels for secure remote communication. The topology is presented in Figure 34 – Reference topology 4 (page 92).

Figure 34 – Reference topology 4



The topology 4 can be implemented with the following components:

- Customer network devices: the same as for topology 1 and 2
- SafeNet IPSec client installed on the remote PC.
- Nortel Eybeam client SMC 3456

Client VPN configuration at main site

1. Create a user account in the BSG8ew local database for the remote tele-workers.
2. Configure the IKE and IPSec SA for client terminations
3. Create an IP address pool for assigning IP addresses to VPN client. The client end of the tunnel should be assigned the following parameters:
   - IP address
   - Netmask
   - Default gateway

- DNS server
- WINS server IP address

Attention: IKE X-AUTH is not supported in Release 1.0

Solution components configuration example

Overview and objective

This section describes the configuration of an actual site in detail. The objective of this section is to present a real world scenario that implements the capabilities of the solution. For the sake of clarity, the example is separated into two topologies, single site topology and site-to-site VPN topology.

Operational assumptions

The following characteristics of the configuration are assumed:

- Switches and access points behind the BSG8ew will be fully configured prior to deployment at customer site.
- The BSG8ew is partially configured in the MSP with following minimum configuration before deploying at customer premises:
  - PPPoE profile (username and password)
  - Firewall rule to allow SSH/Telnet/Http access from MSP
  - Virtual server for SSH/Telnet/Http
- The BSG8ew is to be managed through the http session.
- The Telnet logins to the BSG8ew will be authenticated by TACACS server located within the MSP.
- Critical logs generated by the BSG8ew, BES and BAP will be sent to Syslog server located at the MSP.
- SNTP located within the NOC provides time synchronization services to BSG8ew, BAP and BES.
- The service provider ADSL modem works in bridged mode; that is, the PPPoE session is terminated on the BSG8ew.
- Hosts on the guest VLAN are restricted from reaching the employee data and voice VLANs. They are however granted unfettered access to the Internet.

Single site topology

The typical single site customer configuration is presented in Figure 35 - Customer network topology (page 96). The topology with Site to Site IPSec VPN is presented in the following sections. The topology and provisioning procedure for Site to Site VPN is presented separately in section Site to Site VPN topology (page 160) for the sake of clarity.

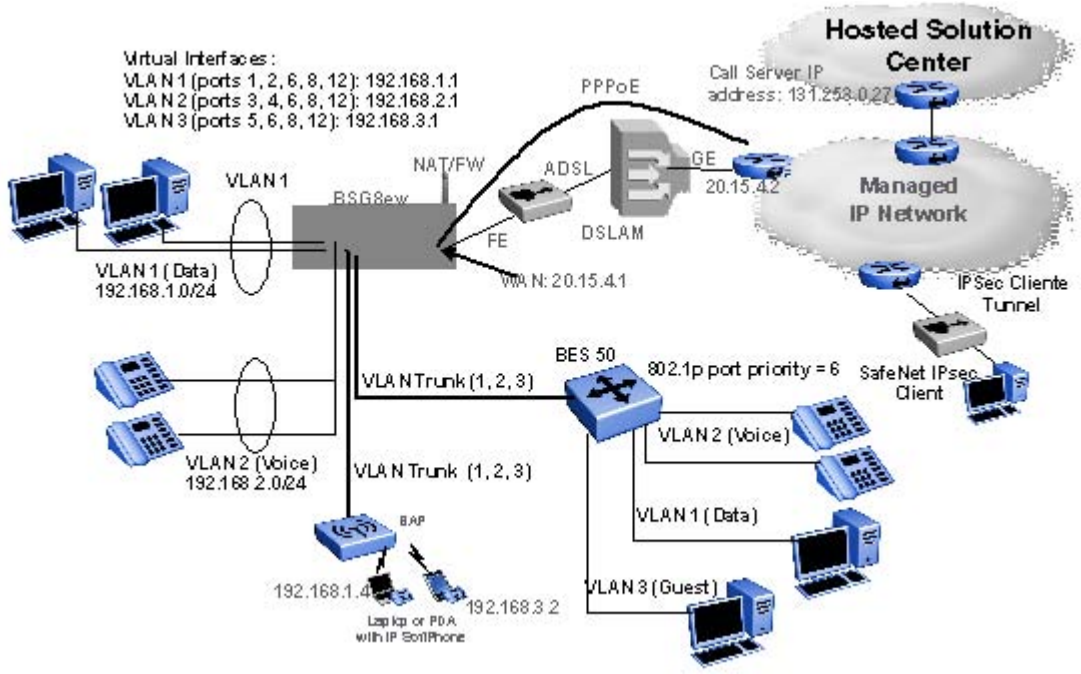
Operating mode

The example topology for the solution is presented in the following figure. The topology consists of:

- 1xBSG8ew
- 1xBES50
- 3xLG 6000 3x
- 2xPC
- 1xBAP 120

The BSG8ew is connected to the service provider network by means of PPPoE tunnel across the DSL connection as presented in the following figure.

Figure 35 - Customer network topology



The BSG8ew has 7 Fast Ethernet ports and one Gigabit Ethernet port. The Fast Ethernet ports are ports 1 through 7. The remaining Ethernet port, port 8 is the Gigabit Ethernet port. In the example, the Fast Ethernet ports are used to connect customer devices, and the Gigabit Ethernet port is used to connect to the BES 50 Ethernet switch.

WAN connectivity

The BSG8ew WAN interface port is connected to the Ethernet port of the ADSL modem that is plugged into the PSTN local loop. The DSL modem is setup to operate in a bridged mode meaning that it is bridging Ethernet frames between BSG8ew and the DSLAM port.

To connect to the Wide Area Network (WAN), a PPPoE protocol is used to establish a PPP session to the BRAS node of the service provider.

LAN connectivity

In the example Gigabit Ethernet port 8 is used to connect to port 12 of BES50GE switch. Port 6 is used to connect to BAP120 Access Point. Ports 1 through 6 are configured as members of three VLANs:

- VLAN 1: ports 1, 2, 6, 8, 12 (Data VLAN)
- VLAN 2: ports 3, 4, 6, 8, 12 (Voice VLAN)
- VLAN 3: port 5, 6, 8, 12 (Guest VLAN)

Port 12 is connected to the BSG8ew's WI-FI device (it is a radio port in CLI). Ports 6 and port 8 are configured as VLAN trunks and they are members of VLAN 1, 2 and 3. Port 6 is connected to BAP120 and port 8 is connected to BES50GE switch.

Wireless LAN

There are three SSIDs configured in the example, one for every customer VLAN:

- SSID Data (VLAN 1)
- SSID Voice (VLAN 2)
- SSID Guest (VLAN 3)

The same SSID to VLAN mapping is provisioned on both BSG8ew and the BAP 120 Access Points.

IP address allocation

The virtual interfaces are pre-configured with the static IP addresses:

- VLAN 1: 192.168.1.1 mask 255.255.255.0
- VLAN 2: 192.168.2.1 mask 255.255.255.0
- VLAN 3: 192.168.3.1 mask 255.255.255.0

DHCP server is enabled and provisioned with three address pools:

- "192.168.1.0/24, default gateway: 192.168.1.1, DNS: 192.168.1.1
- "192.168.2.0/24, default gateway: 192.168.2.1, DNS: 192.168.1.1
- "192.168.3.0/24, default gateway: 192.168.3.1, DNS: 192.168.1.1
- "Reserved IP address 192.168.1.128 for BAP120
- "Reserved IP address 192.168.1.136 for BES50

Required services

This section provides provisioning procedures for the following BSG8ew ata services required to support the network topology:

- PPPoE Client on WAN interface for dynamic IP address assignment
- Customer VLANs: VLAN 1, VLAN 2 and VLAN 3
- DHCP Server with IP address pools to server VLAN 1, VLAN 2 and VLAN 3 devices
- NAT and FW on the WAN interface
- FW on the LAN interface
- Wireless LAN
- IPSec client termination
- SIP proxy
- Call Admission Control
- FXS and FXO interfaces
- QoS

Pre-deployment configuration of BSG8ew

The purpose of this section is to provide configuration steps required to enable remote configuration of the BSG8ew and solution components.

Logging into the BSG8ew

From a PC connected LAN port 1 of the BSG8ew, SSH to 192.168.1.1 and log into the BSG8ew using the default username and password of nnadmin and PlsChgMe! respectively.

WAN configuration

- This deployment uses an ADSL modem for Internet access. The modem must be configured in bridged mode to relay PPPoE frames originated from the BSG8ew onto the DSL link. Please see the modem documentation for instructions.
- The BSG8ew dynamically acquires its WAN IP address using PPP.
- Create a PPP interface and bind it to the WAN port off the BSG8ew. Provide the customer username and password using the following commands:

Provisioning commands:

- `c t`
- `interface fastethernet 0/9`
- `shut`
- `end`
- `c t`
- `interface ppp 1`
- `layer fastethernet 0/9`
- `shut`
- `ppp username user_name password user_password`
- `no shut`

- exit
- interface fastethernet 0/9
- no shut
- end

Virtual server configuration

On the BSG8ew the application servers do not bind to the WAN interface. They only bind to VLAN 1 interface. That means that the packets destined for SSH server need to be forwarded to the VLAN 1 interface. To support this port forwarding capability is required so the packets received on the WAN interface and destined to SSH server (port 22) can be forwarded to VLAN 1 interface. On the BSG8ew this capability is provided by functionality of virtual server

For example, the Telnet as well as the SSH server are behind the NAT on the BSG8ew. To make these services reachable from the MSP virtual servers must be configured on the BSG8ew. The following example shows how this is configured on the BSG8ew. The example assumes that Telnet server listens on port 23 and the SSH server listens on port 22.

- c t
- interface ppp 1
- virtual server 192.168.1.1 23 telnet telnetfromwan
- virtual server 192.168.1.1 22 other 22 sshfromwan
- end

Firewall configuration

Configure the firewall on the BSG8ew to permit connections from telnet, SSH clients located in the MSP. In the example shown below, it is assumed that the IP address of the management console with the clients is 60.50.40.1.

Provisioning commands:

- c t
- firewall
- filter add sshfromwanfil 60.50.40.1/32 192.168.1.1/32 tcp srcport >1 destport =22
- access-list sshfromwanacl in sshfromwanfil permit 71 log brief
- filter add telnetfromwanfil 60.50.40.1/32 192.168.1.1/32 tcp srcport >1 destport =23
- access-list telnetfromwanacl in telnetfromwanfil permit 72 log brief
- end

Password change

For security reasons, it is highly recommended that the password of the administrator account on the BSG8ew is changed. Use the following command to change the password of the nnadmin account:

Provisioning commands:

- `c t`
- `username nnadmin password my123$#password nnadmin`
- `end`

Write configuration to flash memory:

Provisioning command:

- `write startup-config`

Power down the BSG8ew

Post installation configuration of BSG8ew

Customer VLANs creation

VLAN 1 (Data VLAN)

- `cas# configure terminal`
- `cas(config)# vlan 1`
- `cas(config-vlan)# ports fastethernet 0/1-2 0/6 gi 0/8 radio 1/1 untagged fastethernet 0/1-2 name Data`
- `cas(config-vlan)# end`

VLAN 2 (Voice VLAN)

- `cas# configure terminal`
- `cas(config)# vlan 2`
- `cas(config-vlan)# ports fastethernet 0/3-4 0/6 gi 0/8 radio 1/1 untagged fastethernet 0/3-4 name Voice`
- `cas(config-vlan)# exit`
- `cas(config)# interface fastethernet 0/3`
- `cas(config-if)# switchport pvid 2`
- `cas(config-if)# no shutdown`
- `cas(config-if)# exit`
- `cas(config)# interface fastethernet 0/4`

- `cas(config-if)# switchport pvid 2`
- `cas(config-if)# no shutdown`
- `cas(config-if)# end`

VLAN 3 (Guest VLAN)

- `cas# configure terminal`
- `cas(config)# vlan 3`
- `cas(config-vlan)# ports fastethernet 0/5-6 gi 0/8 radio 1/1  untagged fastethernet 0/5 name Guest`
- `cas(config-vlan)# exit`
- `cas(config)# interface fastethernet 0/5`
- `cas(config-if)# switchport pvid 3`
- `cas(config-if)# no shutdown`
- `cas(config-if)# end`

NOTE: A switchport command is required to move the port from one VLAN to another. For example if the port is a member of VALN 1 (a default VLAN) and VLAN ports command is used to add the port to VLAN 3, the port is not removed from VLAN 1. In order to make the port member of VLAN 3 only, a switch command needs to be executed to remove the port from VLAN 1.

Virtual interfaces

A virtual interface associated with the VLAN must be configured to provide routed service to members of the VLAN. By default there is already a default VLAN interface with IP address 192.168.1.1/24 associated with VLAN 1, the VoIP VLAN. Use the following commands to create virtual interface for VLAN 2 and VLAN 3 and assign it IP address of 192.168.2.1/24 and 192.168.3.1/24 respectively.

Table 22 - BSG8ew VLAN to subnet mapping

VLAN / VLAN name	VLAN IP
VLAN 1 / Data	192.168.1.1/24
VLAN 2 / Voice	192.168.2.1/24
VLAN 3 / Guest	192.168.3.1/24

Provisioning commands:

- `c t`
- `interface vlan 2`
- `ip address 192.168.2.1 255.255.255.0`
- `no shut`

- `exit`
- `interface vlan 3`
- `ip address 192.168.3.1 255.255.255.0`
- `no shut`
- `end`

DHCP server IP address pools

By default, a single DHCP scope is configured on the BSG8ew associated with VLAN 1. This scope needs to be augmented to reserve some IP addresses for hosts that must be assigned fixed addresses. Two additional DHCP scopes must be defined to serve DHCP clients that will be connected to the Voice and Guest VLANs. Table 23 summarizes the new configuration of the two scopes on the BSG8ew.

Table 23 DHCP Server configuration

Scope name	DHCP option	Reserved IP address / device
Pool 1 / Data	Range: 192.168.1.2 - 192.168.1.127 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1 DNS: 192.168.1.1	192.168.1.128 / BES50 192.168.1.136 / BAP120
Pool 2 / Voice	Range: 192.168.2.2 - 192.168.2.127 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.2.1 DNS: 192.168.1.1	
Pool 3 / Guest	Range: 192.168.3.2 - 192.168.3.127 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.3.1 DNS: 192.168.1.1	

Since the LAN may have both dynamically and statically configured hosts on the LAN, the possibility of duplicate IP address exists. To avoid this, configure the BSG8ew to ping an IP address prior to assigning it to a DHCP client.

Reserve two IP addresses in the Data VLAN for the BAP120 and BES50.

Provisioning commands:

- `cas# configure terminal`
- `cas (config)# ip dhcp ping packets`
- `cas(config)# ip dhcp pool 1`
- `cas(dhcp-config)# network 192.168.1.0 / 24 192.168.1.127`

- `cas(dhcp-config)# host hardware-type 1 client-identifier 00:11:22:33:44:55 ip 192.168.1.136 BAP120`
- `cas(dhcp-config)# host hardware-type 1 client-identifier 66:77:88:99:10:11 ip 192.168.1.128 BES50`
- `cas(dhcp-config)# default-router 192.168.1.1`
- `cas(dhcp-config)# dns-server 192.168.1.1`
- `cas(dhcp-config)# lease 0 7 0`
- `exit`
- `cas(config)# ip dhcp pool 2`
- `cas(dhcp-config)# network 192.168.2.0 / 24 192.168.2.127`
- `cas(dhcp-config)# default-router 192.168.2.1`
- `cas(dhcp-config)# dns-server 192.168.1.1`
- `cas(dhcp-config)# lease 0 7 0`
- `cas(dhcp-config)# end`
- `cas# show ip dhcp server pools`

- `cas# configure terminal`
- `cas(config)# ip dhcp pool 3`
- `cas(dhcp-config)# network 192.168.3.0 / 24 192.168.3.127`
- `cas(dhcp-config)# default-router 192.168.3.1`
- `cas(dhcp-config)# dns-server 192.168.1.1`
- `cas(dhcp-config)# lease 0 7 0`
- `cas(dhcp-config)# end`
- `cas# show ip dhcp server pools`

Note: DNS Server is reachable only through the VLAN 1 virtual interface IP address (in the example it is 192.168.1.1).

Firewall

- It is assumed that employees (Data VLAN 1) of the customer are given unfettered access to the Internet. Delete all the factory default firewall rules and add a rule to allow all hosts on VLAN 1 to be able to reach a service over the WAN interface.
- Add a firewall rule to allow hosts on VLAN 2 (Voice), to be able to access any service on any host on the WAN side of the BSG8ew.
- Add a rule to deny hosts on the Guest VLAN 3 from reaching the Voice VLAN and Data VLAN.
- Convert the virtual interface associated with the Guest VLAN 3 into untrusted port and configure firewall rule to deny members of the Guest VLAN 3 from services on the Data VLAN 1.

- Also add a rule to allow members of the Guest VLAN 3 to have full access to services over the WAN interface.
- Add a rule to permit member of Guest VLAN 3 to be able to send DNS queries to the DNS server on the BSG8ew which is using an IP address of 192.168.1.1
- Add rule to prevent members of Guest VLAN 3 from being able to Telnet, SSH, HTTP and HTTPS to the BSG8ew.
- Add a firewall rule to allow remote access VPN from remote Safenet client. The rule must allow IKE and ESP exchanges between remote clients and the BSG8ew.

Also add a rule to allow remote VPN clients to get access to IP services available to the Data VLAN 1.

Provisioning commands:

- `c t`
- `firewall`
- `no access-list Def_FTP_ACL out`
- `no access-list Def_TELNET_ACL out`
- `no access-list Def_SMTP_ACL out`
- `no access-list Def_DNS_TCP_ACL out`
- `no access-list Def_DNS_UDP_ACL out`
- `no access-list Def_HTTP_ACL out`
- `no access-list Def_HTTPS_ACL out`
- `no access-list Def_POP3_ACL out`
- `no access-list Def_IMAP_ACL out`
- `no access-list Def_SNTP_ACL out`
- `no filter Def_FTP_Filter`
- `no filter Def_TELNET_Filter`
- `no filter Def_SMTP_Filter`
- `no filter Def_DNS_TCP_Filter`
- `no filter Def_DNS_UDP_Filter`
- `no filter Def_HTTP_Filter`
- `no filter Def_HTTPS_Filter`
- `no filter Def_POP3_Filter`
- `no filter Def_IMAP_Filter`
- `no filter Def_SNTP_UDP_Filter`

- `filter add vlan1_2_anywhere_filter 192.168.1.0/24 any any srcport >1 destport >1`
- `access-list vlan1_2_anywhere_acl out vlan1_2_anywhere_filter permit 1000 log brief`

- `filter add vlan2_to_anywhere_filter 192.168.2.0/24 any any srcport >1 destport >1`
- `access-list vlan2_to_anywhere_acl out vlan2_to_anywhere_filter permit 1001 log brief`

- `filter add guest2vlan1fil 192.168.3.0/24 192.168.1.0/24 any srcport >1 destport >1`
- `access-list guest2vlan1acl in guest2vlan1fil deny 60 log brief`

- `filter add guest2vlan2fil 192.168.3.0/24 192.168.12.0/24 any srcport >1 destport >1`
- `access-list guest2vlan1acl in guest2vlan1fil deny 61 log brief`

- `untrusted port vlan 3`

- `filter add guestdnsfil 192.168.3.0/24 192.168.1.1/32 udp srcport >1 destport =53`
- `access-list guestdnsacl in guest2dnsfil permit 59 log brief`
- `filter add guesttelnetmgmfil 192.168.3.0/24 192.168.3.1/32 tcp srcport >1 destport =23`
- `access-list guesttelnetmgmacl in guesttelnetmgmfil deny 58 log brief`
- `filter add guesthttpmgmfil 192.168.3.0/24 192.168.3.1/32 tcp srcport >1 destport =80`
- `access-list guesthttpmgmacl in guesthttpmgmfil deny 57 log brief`
- `filter add guestsshmgmfil 192.168.3.0/24 192.168.3.1/32 tcp srcport >1 destport =22`
- `access-list guestsshmgmacl in guestsshmgmfil deny 56 log brief`
- `filter add guesthttpsmgmfil 192.168.3.0/24 192.168.3.1/32 tcp srcport >1 destport =443`
- `access-list guesthttpsmgmacl in guesthttpsmgmfil deny 55 log brief`

- `filter add guest2wanfil 192.168.3.0/24 0.0.0.0/00 any srcport >1 destport >1`
- `access-list guest2wanacl out guest2wanfil permit 2000 log brief`

- `filter add  ikefromWANfil any any other UDP srcport >1 destport =500`
- `access-list ikefromWANacl in ikefromWANfil permit 2001 log brief`

- `filter add espfromWANfil any any other 50 permit srcport >1 destport >1`
- `access-list espfromWANacl in espfromWANfil permit 2002 log brief`
- `end`

Wireless LAN configuration

Factory default settings on the BSG8ew have one SSID configured which is disabled. This cannot be renamed and must first be deleted before new SSIDs can be added. Three new SSIDs must be configured. First SSID provides data services to employees of the customer, second SSID provide wireless access to the SIP soft clients and third SSID provides guest access. It is highly recommended to use at least WPA-PSK to secure all SSIDs. Ensure that the pre-shared key configured for employees is different from that configured for guest users.

- Map the Data SSID to VLAN 1, Voice SSID to VLAN 2 and the Guest SSID to VLAN 3.
- For added security disable the capability to broadcast the configured SSIDs.
- Once all the SSIDs have been configured, select the country code representing the country in which the BSG8ew is installed prior to enabling the radio.

Table 24 SSID Configuration

SSID	VLAN ID	Authentication	Pairwise and Group Cipher
Data	1	WPA-PSK	TKIP
Voice	2	WPA-PSK	TKIP
Guest	3	WPA-PSK	TKIP

Provisioning commands:

- `c t`
- `config wlan delete 1`
- `config wlan create 1 Data`
- `config wlan security auth-type wpa-psk 1`
- `config wlan security cipher-suite tkip 1`
- `config wlan security pre-shared-key 1 ascii data`
- `config wlan broadcast-ssid disable 1`
- `config wlan interface 1 vlan1`
- `config wlan enable 1`

- `config wlan create 2 Voice`
- `config wlan security auth-type wpa-psk 2`
- `config wlan security cipher-suite tkip 2`
- `config wlan security pre-shared-key 2 ascii voice`

- `config wlan broadcast-ssid disable 2`
- `config wlan interface 2 vlan2`
- `config wlan enable 2`

- `config wlan create 3 Guest`
- `config wlan security auth-type wpa-psk 3`
- `config wlan security cipher-suite tkip 3`
- `config wlan security pre-shared-key 3 ascii guest`
- `config wlan broadcast-ssid disable 3`
- `config wlan interface 3 vlan3`
- `config wlan enable 3`

- `config ap country us`
- `interface radio 1/1`
- `config dot11 enable network`
- `end`

SIP proxy configuration

The steps below summarize the process of configuring the BSG8ew SIP proxy:

- Determine the IP address assigned to the VoIP1K chip on the BSG8ew (use CLI "show sub-system information" command).
- Determine the emergency number for your jurisdiction and configure BSG8ew to route calls to the emergency via the FXO port to the PSTN. This requires editing the normal mode dial plan file and downloading the file to the BSG8ew using FTP. See below for a sample of the normal mode dial plan. It assumes the IP address of the VoIP1K is 192.168.1.2.
- Similarly, configure the BSG8ew to route emergency calls via the FXO port to the PSTN in a backup mode. As in the normal mode, this is done, by editing the backup dial plan and downloading the file to the BSG8ew using FTP. See below for a sample of the backup mode dial plan configured to route emergency calls via the PSTN. Again, it assumes the IP address of the VoIP1K is 192.168.1.2
- FTP the normal and backup mode dial plans to the BSG8ew (FTP Server IP address is 131.253.0.28)
- Configure the IP address of the MSP managed SIP server. In this example IP address of the SIP server is 131.253.0.27
- Configure Home Domain of the SIP server
- Configure BSG8ew to use UDP as the transport protocol used between the BSG8ew and SIP.
- Configure the polling interval, the number of retries for each poll and the poll timeout.
- Delete both the current normal and backup dial plans.
- Configure the BSG8ew to use the new normal and backup dial plans just downloaded.
- Reload all the dial plans.

Sample normal mode dial plan:

```
<!-- Global plan for normal mode -->
<translation>
 <address-switch field="previoushop">
    <address is="131.253.0.27">
     </address>
     <otherwise>
       <number-switch>
      <number prefix="911">
         <route host="192.168.1.2" port="5060" replace-host="yes"/>
      </number>
      <otherwise>
         <route host="131.253.0.27" transport ="udp" port="5060"
replace-host="no" add-route="yes"/>
      </otherwise>
      </number-switch>
      </otherwise>
</address-switch>


Sample Backup Mode Dial Plan:


<!-- Global plan for backup mode -->
<translation>
    <number-switch>
    <number prefix="911">
          <route host="192.168.1.2" transport ="udp" port="5060"
replace-host="no" add-route="yes" />
      </number>
</number-switch>
</translation>
```

Provisioning commands:

- `copy ftp ftpusername ftppassword 131.253.0.28 normalglobaldialplan.xml normalglobaldialplan.xml`
- `copy ftp ftpusername ftppassword 131.253.0.28 backupglobaldialplan.xml backupglobaldialplan.xml`
- `c t`
- `sip`

- `delete dialplan normalglobaldialplan`
- `delete dialplan backupglobaldialplan`
- `add dialplan normalglobaldialplan normalglobaldialplan.xml`
- `add dialplan backupglobaldialplan backupglobaldialplan.xml`
- `reload dialplan all`
- `dialplan`
- `set sipserver NormalModeGlobalDialPlanName normalglobaldialplan`
- `set sipserver BackupModeGlobalDialPlanName backupglobaldialplan`
- `exit`
- `domain`
- `set sipserver polledservers pollingaddress 131.253.0.27 port 5060 pollinginterval 300 pollretries 3 transport udp`
- `set serverdomainname nortel.com`
- `exit`
- `end`

Call Admission Control

The following procedure can be used to calculate and configure CAC on the BSG8ew:

- Determine the uplink bandwidth of the BSG8ew WAN interface. In this example, it is assumed the BSG8ew is connected to the WAN via an ADSL modem with an uplink of 500 Kbps.
- Determine the bandwidth requirement of the CODEC that will be used by the sets. Table below shows voice channel bandwidth for the different CODECs.
- Determine the fraction of uplink bandwidth that should be reserved for VoIP traffic across the WAN interface. Keep in mind that a certain fraction of the uplink bandwidth should be reserved for data.
- Assuming that 60 % of the uplink is going to be guaranteed for VoIP traffic, 20% to employee data traffic and 10% to guest data traffic, the table below shows the maximum number of simultaneous WAN calls that can be supported for the different CODECs.

	Frame Duration in ms (payload)	**Voice Payload (bytes)**	**IP Packet (bytes)**	**Ethernet Frame (bytes)**	**Ethernet Bandwidth in Kbps**	**Bandwidth Reserved for VoIP**	**CAC**
G.711 (64Kbps)	10	80	120	154	123.2	300	2
	20	160	200	234	93.6	300	3
	30	240	280	312	83.2	300	3
G.729A/ G.729 (8 Kbps)	10	10	50	84	67.2	300	4

	20	20	60	94	37.6	300	8
	30	30	70	104	27.7	300	11

The following commands configure maximum number of simultaneous calls to be 8:

- `c t`
- `sip`
- `cas`
- `set sipserver maximumSimWANCallsAllowed ppp1 8`
- `end`

FXS configuration

- isable the VoIP1K
- Set the default CODEC for the VoIP to g729 with frame size of 20 ms, g711u with preference of 2 frame duration of 20ms and g711A with preference of 3 and frame duration of 20 ms.
- Set the time offset with respect to GMT
- It is assumed that one of the FXS ports, port 1 will be used for telephony and second port will be used for FAX services.
- Configure FXS port 1 for telephony with the following:
  - The channel (phone) number
  - Configure password for port 1
  - Configure display name
  - Set the CODEC to G.729 and frame duration to 20 ms as the first preference, , g711u with second preference with frame duration of 20ms and g711A as third preference and frame duration of 20 ms.
  - Enable the CODEC status. This allows the FXS to use the preference assigned to the CODECs above rather than default settings.
  - Enable FXS port 1
- Configure FXS port 2 for FAX services with the following:
  - The channel (phone) number
  - Configure password for port 2
  - Configure display name
  - Enable the FAX service on this line and indicate that the port is used exclusively for FAX.
  - Enable FXS port 2
  - Re-enable the VoIP1000

Provisioning commands:

- `c t`
- `voip`
- `shutdown`

- `set default codec type g729 preference 1 frame size 20`
- `set default codec type g711u preference 2 frame size 20`
- `set default codec type g711a preference 3 frame size 20`
- `set gmt-offset -4`
- `exit`
- `interface fxs channel 1`
- `set fxs channel-number 6137634121`
- `set fxs password mypassword`
- `set fxs display-name "John Doe"`
- `set fxs codec type g729 preference 1 frame size 20`
- `set fxs codec type g711u preference 2 frame size 20`
- `set fxs codec type g711a preference 3 frame size 20`
- `set fxs codec status enable`
- `set fxs line enable`
- `exit`
- `interface fxs channel 2`
- `set fxs channel-number 6137634122`
- `set fxs password myfaxpassword`
- `set fxs display-name "John Doe"`
- `set fxs fax-option foip-voice`
- `set fxs line enable`
- `exit`
- `voip1000`
- `no shut`
- `end`

FXO configuration

- Disable the VoIP1000
- Configure the FXO port with the phone number of the PSTN line
- Set the emergency number for your local area. This is needed such that when there is contention between a non-emergency call and an emergency call via the PSTN, the FXO gives priority to the emergency call.
- Configure the FXO with the phone number to which all calls from the PSTN will be forwarded. Ideally, this number should be belong to one of the SIP sets that will be connected to the LAN side of the BSG8ew.
- Set the number of times that the FXO should ring before the call is forwarded to the above number.
- Enable the FXO port as PSTN Gateway.
- Re-enable the VoIP1000.

Provisioning commands:

- `c t`
- `voip1000`
- `shutdown`
- `exit`
- `interface fxo channel 1`
- `set fxo channel-number 6137633894`
- `set fxo emergency-number 911`
- `set fxo forward phone-no sipline9199999036`
- `set fxo ring count 1`
- `set pstn-gateway enable`
- `exit`
- `voip1000`
- `no shut`
- `end`

QoS configuration

- Create three classifier rules to classify all ingress LAN traffic into four broad categories:
  - Data Traffic from Data VLAN
  - Guest Traffic from Guest VLAN
  - Voice Traffic from Voice VLAN
- Configure the TRTCM policer to commit 60% of the uplink WAN bandwidth to the voice traffic. The assumed uplink bandwidth is 500 kbps. The policer should also be configured to police the voice traffic at 60% of nominal uplink bandwidth.
- Configure the policer to guarantee traffic from the Data VLAN 30% of the uplink WAN bandwidth. However, in the absence of congestion, the policer should be configured to allow the Data VLAN traffic to burst up 100% of available uplink WAN bandwidth.
- Similarly, policer is configured to guaranteed traffic from Guest VLAN of remaining bandwidth (10%) but allow to burst up to 100% of uplink bandwidth in the absence of congestion.

Table 25 Policer configuration

Flow	Committed information rate (% of uplink bandwidth)	Peak information rate (% of uplink bandwidth)
Data Traffic	30	100
Guest Traffic	10	100
Voice Traffic	60	60

- Configure the Marker to mark traffic from the employee Data VLAN with 802.1p user priority of 5 and DSCP value of AF31. This maps employee data traffic to queue number 3 .
- Configure the Marker to mark traffic from the Guest VLAN with 802.1p user priority of 4 and DSCP value of AF21. This maps Guest traffic to queue number 4.
- Configure the Marker to mark traffic from the Voice VLAN with 802.1p user priority of 6 and DSCP value of EF. This effectively maps voice traffic to queue number 1 of egress queues on the WAN port..
- Configure the BSG8ew to use WRR to scheduling the Data and Guest VLAN traffic with more bandwidth assigned to the employee data traffic. This is done by assigning a weight of 48 and 24 to queue 5 and 4 respectively.
- Assign a minimum and maximum threshold for Yellow colored packets of 75 and 100 respectively to queues 1, 3 and 4.
- Assign a minimum and maximum threshold for Yellow colored packets of 250 and 350 respectively to queue number 3 and 4.

Table 26 Marker and Queue Configuration

Flow	802.1p Priority	DSCP	Egress Queue	Weight	Min. Green Threshold	Max. Green Threshold	Min. Amber Threshold	Max Amber Threshold
Voice	6	EF (46)	1	0	100	100	100	100
Employee Data	5	AF31(26)	2	48	250	350	75	100
Guest Data	4	AF21(18)	3	24	250	350	75	100

Provisioning commands:

- `c t`
- `class-map 1 permit source-net 192.168.1.0 255.255.255.0 dest-net 0.0.0.0 0.0.0.0`
- `class-map 2 permit source-net 192.168.2.0 255.255.255.0 dest-net 0.0.0.0 0.0.0.0`
- `class-map 3 permit source-net 192.168.3.0 255.255.255.0 dest-net 0.0.0.0 0.0.0.0`

- police 1 type trtcm pir 500000 cir 150000 pbs 3000 cbs 3000
- police 2 type trtcm pir 300000 cir 300000 pbs 3000 cbs 3000
- police 3 type trtcm pir 500000 cir 50000 pbs 3000 cbs 3000
- policy-map 1 class 1
- policy-map 2 class 2
- policy-map 3 class 3
- class 1 set ip dscp 26 priority 5
- class 2 set ip dscp 46 priority 6
- class 3 set ip dscp 18 priority 4
- interface fastethernet 0/9
- queue weight 3 48
- queue weight 4 24
- queue threshold 1 100 100 100 100
- queue threshold 3 250 350 75 100
- queue threshold 4 250 350 75 100
- end

TACACS and logging authentication

CLI may be used to manage BSG8ew. For scalability reasons, it is assumed that credentials of users logging into the BSG8ew are created on a central database that is accessible to a TACACS and server located at the MSP. The BSG8ew should also be configured to use local database to authenticate an SSH session should the TACACS server be unavailable.

Enable TACACS and authentication and configured BSG8ew to use local database in case the TACACS and server is offline.

Configure the BSG8ew with the IP address and shared secret of the TACACS+ server.

Provisioning commands

- c t
- login authentication tacacs fallback_to_local
- tacacs-server host 60.50.40.4 port 49 timeout 5 key secret
- tacacs-server retransmit 3
- end

IPSec client termination

- The VPN feature is disabled by default, so first enable it.
- Create accounts for 6 remote access VPN users on the BSG8ew.
- Define an IP address pool from which an IP address will be assigned to a remote user as a trusted IP.
- Now define your VPN policy and bind it the WAN interface of the BSG8ew.

- — Set the key mode to xauth
- — Configure IPSec mode as tunnel
- — Set the peer type identity and provide the email address that will be used by all remote VPN clients. In this example, all remote VPN clients will initially be using ra_user@stolbergblanquette.com as their identity.
- — Similarly, set the local identity type to fqdn and provide the FDQN of the BSG8ew.
- — Configure BSG8ew to use preshared key to authenticate phase 1 and provide the value of the preshared key. This preshared key must be configured on all remote VPN clients.
- — Provide the security policy for protecting IKE exchanges between BSG8ew and remote clients
- — Provide the security policy for protecting ESP exchanges between IPSec clients and the BSG8ew.
- — Now configure the access list for which the above security policy should be applied. Here you want anything from Data VLAN (192.168.1.0/24) destined to secure IP address of remote VPN clients to be protected by configured policy

Finally apply the configured VPN policy to your WAN interface.

```
c t
set vpn enable
ra-vpn username user1 password password1
ra-vpn username user2 password password2
ra-vpn username user3 password password3
ra-vpn username user4 password password4
ra-vpn username user5 password password5
ra-vpn username mspadmin password mspadmin


ip local pool clientterminationpool  192.168.4.1-192.168.4.8


# VPN Policy
#=====================================================================
crypto map vpnclienttermination
crypto key mode xauth
crypto ipsec mode tunnel
isakmp peer identity email ra_user@stolbergblanquette.com
set local identity ipv4 46.129.66.70
isakmp policy authentication preshared ravpnpassword
isakmp policy encryption aes-192  hash sha1 dh group2 exch aggressive
lifetime secs 360000
crypto map ipsec encryption esp aes-192 authentication esp sha1 pfs
group2 lifetim secs  3600
```

- `access-list apply any source 192.168.1.0 255.255.255.0 destination 192.168.4.0 255.255.255.0`
- `exit`
- `interface ppp 1`
- `crypto map vpnclienttermination`
- `end`

Software upgrades

The software upgrade of the BSG8ew requires downloading of the new software image and rebooting the BSG8ew to activate the new image. The following commands can be executed to download the new software from the ftp server (IP address of ftp server is 20.0.0.100) :

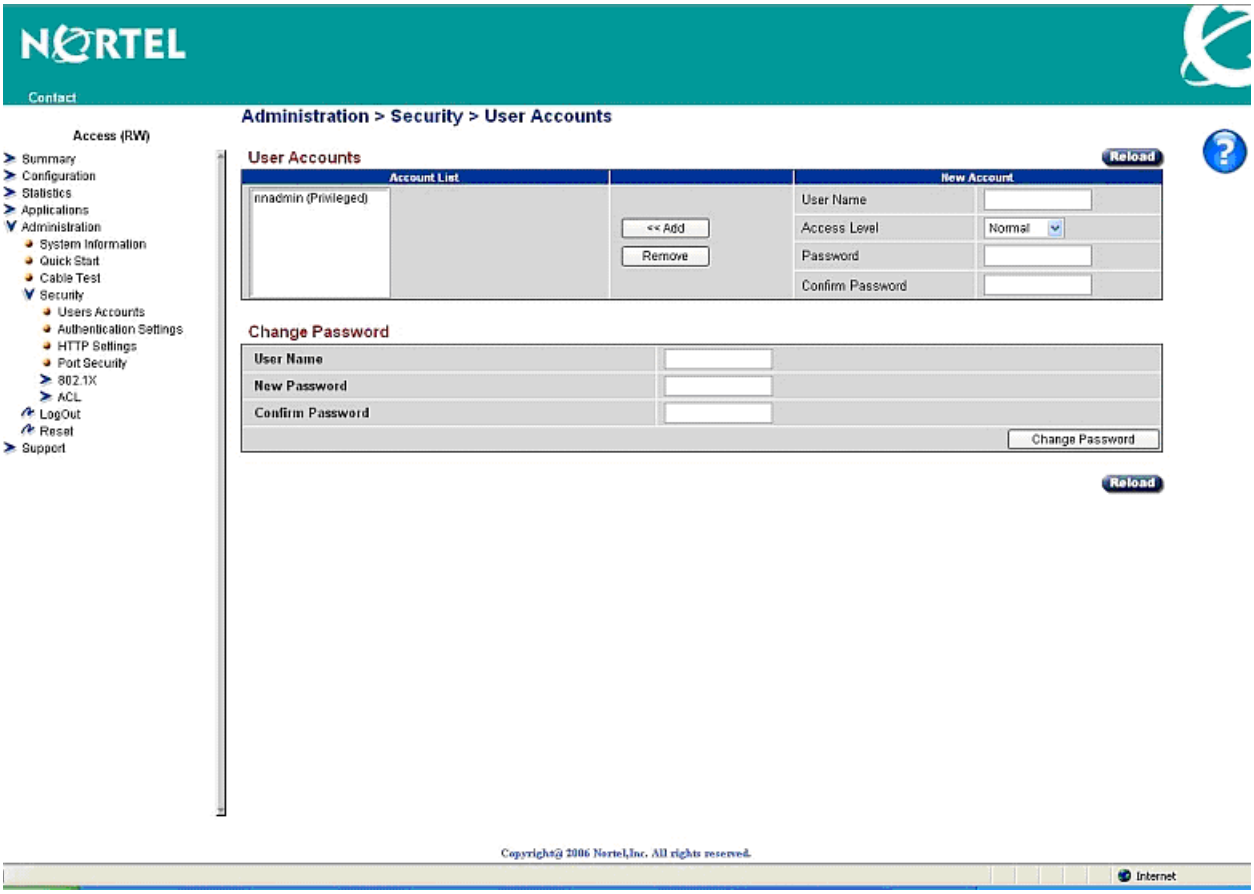
- `c t`
- `archive download-sw /leave-old-sw tftp 20.0.0.100 filename.save`

Pre-deployment configuration of BES50

User management configuration

- Configure the network interface card of a PC with IP address 192.168.1.1/24 and connect it to port 2 of the BES50.
- Point your browser http://192.168.1.128 and log onto the BES50 using the default username and password of *nnadmin* and *PlsChgMe!* respectively.
- Change the password of the default username.
  - From the left hand side menu tree, navigate to the item Administration > Security > User Accounts to bring up the User Accounts panel.
  - Under the Change Password section, type in the default username *nnadmin* in the User Name entry box.
  - Type in the new password in the New Password entry box.
  - Re-type the new password in the Confirm Password entry box to ensure the password is correct.
  - Click on the Change Password button to change the password.

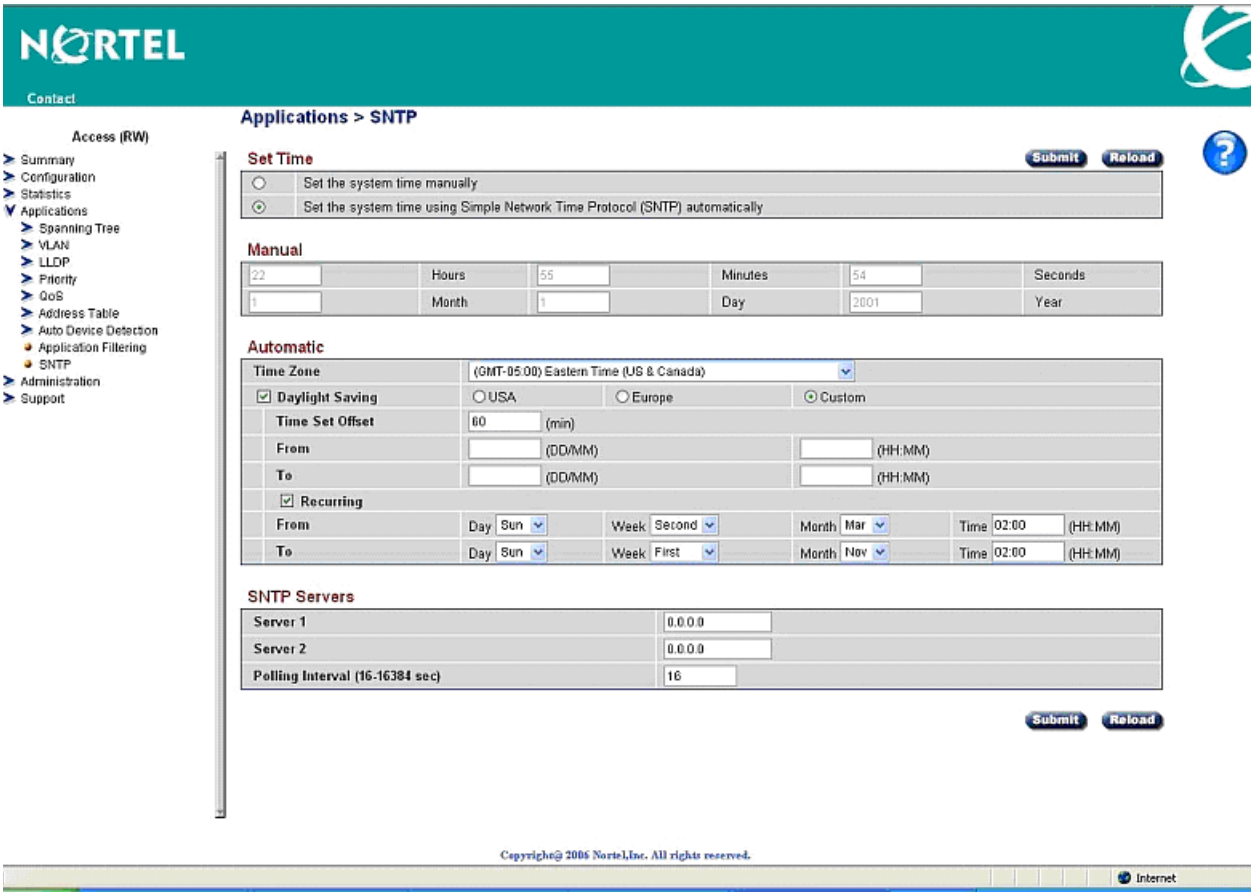
User management configuration



Network management related OAM configuration

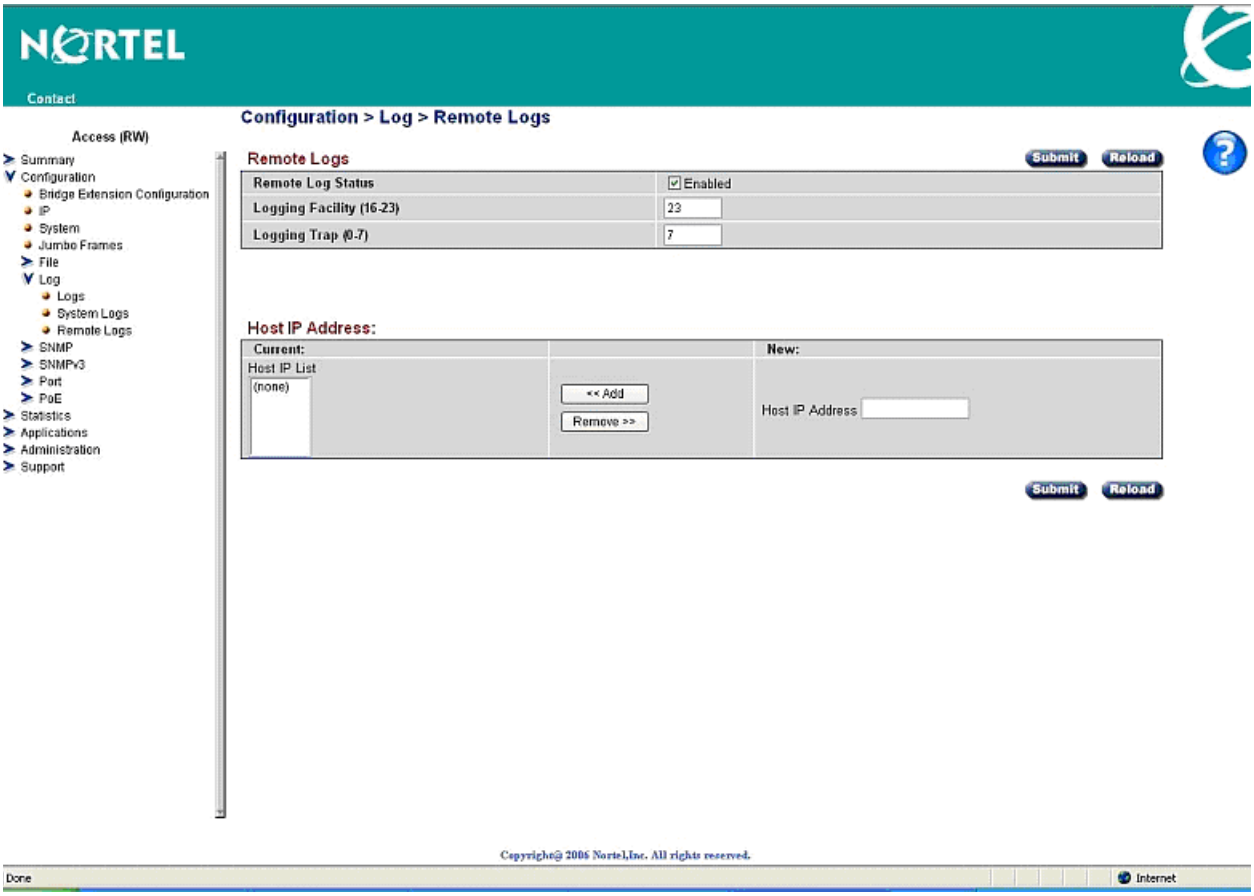
- Configure the BES50 to use the SNTP server located in the MSP network.
  - From the left hand side menu tree, navigate to the item Applications > SNTP to bring up the SNTP panel.
  - Under the Set Time section, click on the radio button to set the system time using SNTP.
  - From the Time Zone drop down menu, select the appropriate time zone where the BES50 is deployed.
  - Check the Daylight Saving checkbox if Daylight Saving Time is needed in the deployment, also configure the appropriate daylight saving time period.
  - Under the SNTP Servers section, fill in the IP address of the SNTP server in the Server 1 entry box.
  - Click on the Submit button to apply the changes.

Network management related OAM configuration



- Configure the BES50 to use the Syslog server located in the service provider network.
  - From the left hand side menu tree, navigate to the item Configuration > Log > Remote Logs to bring up the Remote Logs panel.
  - Under the Remote Logs section, click on the checkbox to enable remote system log.
  - Under the Host IP Address section, fill in the syslog server IP address in the Host IP Address entry box.
  - Click on the Add button to add new syslog server to BES50.
  - Click on the Submit button to enable remote logging.

Remote logs



VLAN configuration

- By default, all the ports of the BES50 are members of a VLAN 1.
- Modify the VLAN membership of the ports to reflect the customer premises deployment as summarized in below:

Table 7 BES50 Port VLAN membership

	VLAN 1 (Data)	VLAN 2 (Voice)	VLAN 3 (Guest)
Untagged Ports	13-18	1-12	19 - 22
Tagged Ports	23 and 24	23 and 24	23 and 24

- Create new Guest VLAN 3 (steps shown for Gust VLAN).

— From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Static List to bring up the Static List panel. This panel manages the VLAN currently configured on BES50. (Note that the name of VLAN 1 is defaultVLAN, which needs to change later on).

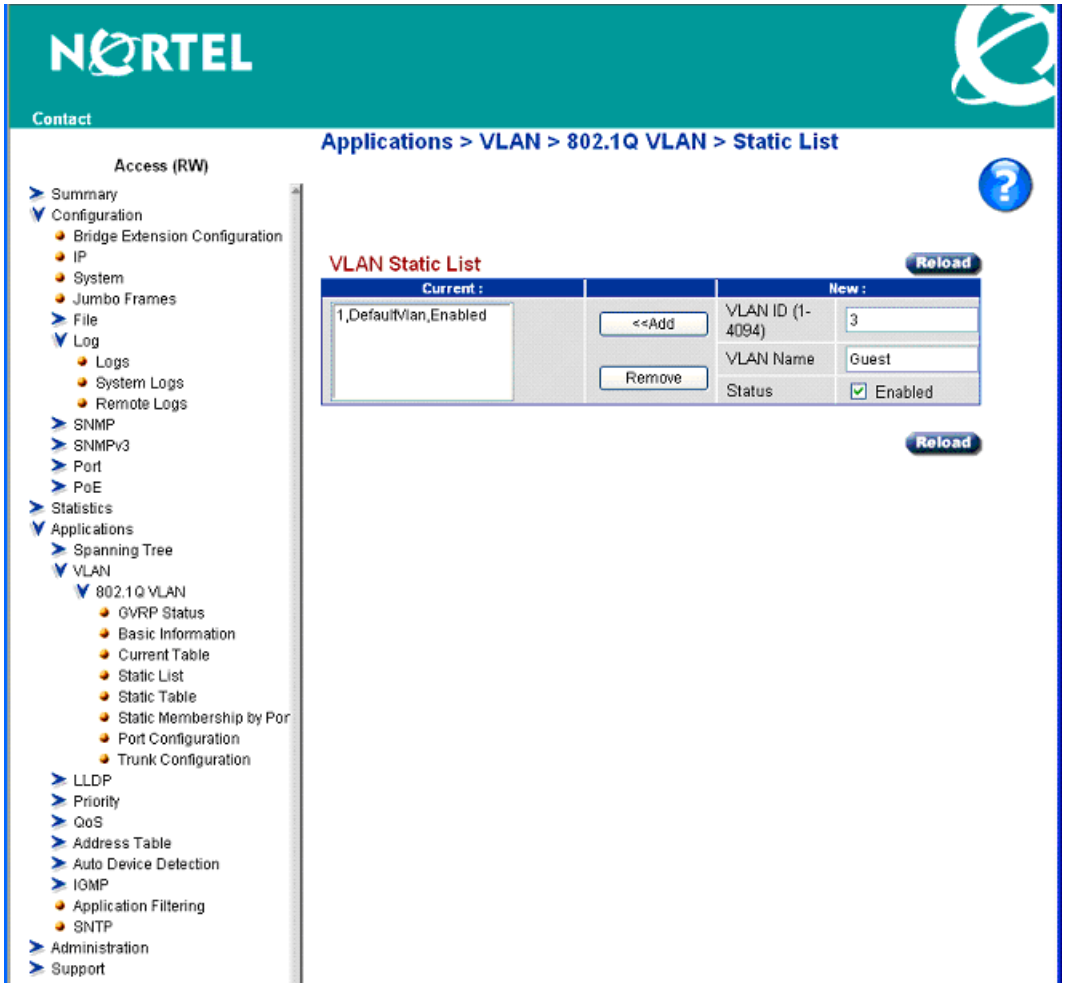
— Under the VLAN Static List section, fill in the value *3* in the VLAN ID entry box.

— Fill in the name Guest in the VLAN Name entry box.

— Check the Status checkbox to enable the newly configured VLAN.

— Click on the Add button to add the new VLAN to BES50.

VLAN static list



- Configure Port 23 and 24 as Tagged member of VLAN3 (Guest VLAN).
- Configure Port 19-22 as Untagged member of VLAN3 (Guest VLAN).
- All other ports are not member of VLAN3 (Guest VLAN).

— From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Static Table to bring up the Static Table panel. This panel manages the port membership of a specified VLAN, and the egress behavior of the membership ports.

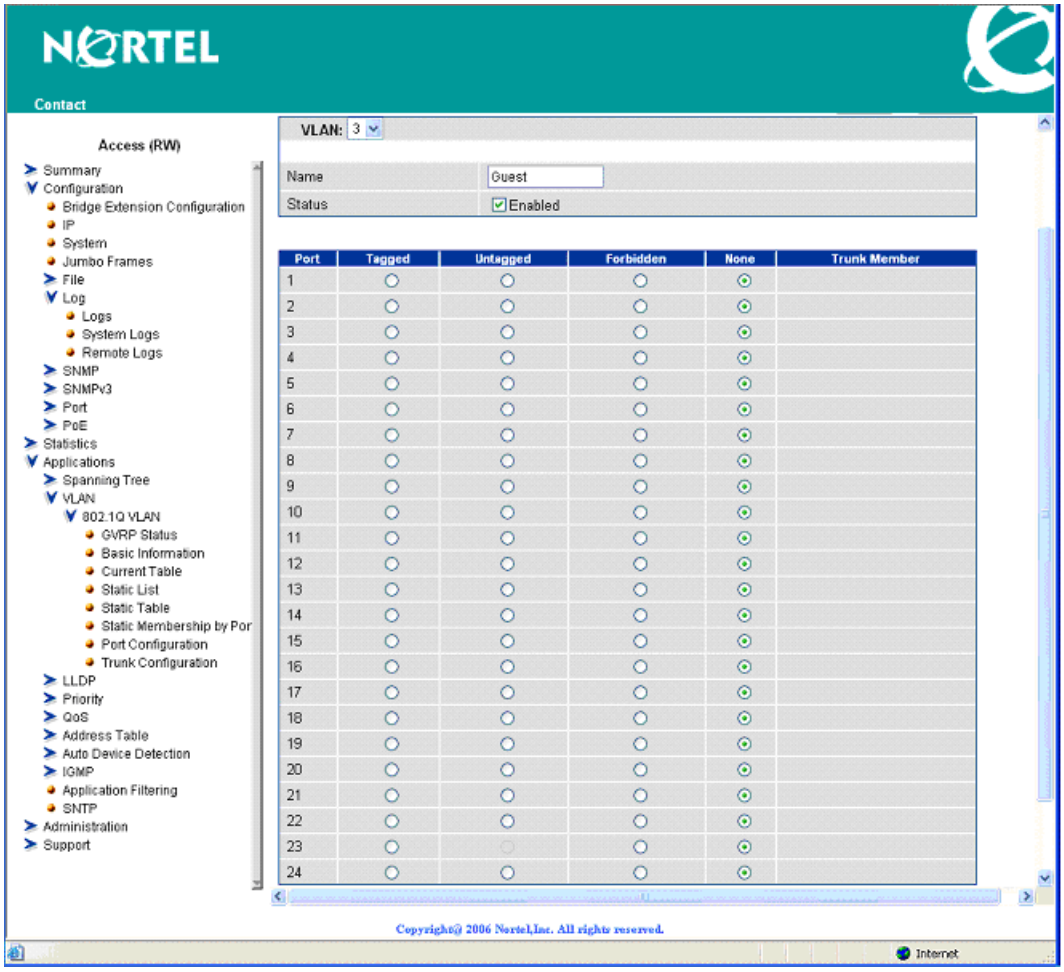
— Under the VLAN Static Table section, select VLAN ID 3 from the VLAN drop down menu. Once VLAN 3 is selected, the panel will refresh to show the current port membership of VLAN 3. By default, none of the ports is member of a newly created VLAN (see the first screenshot).

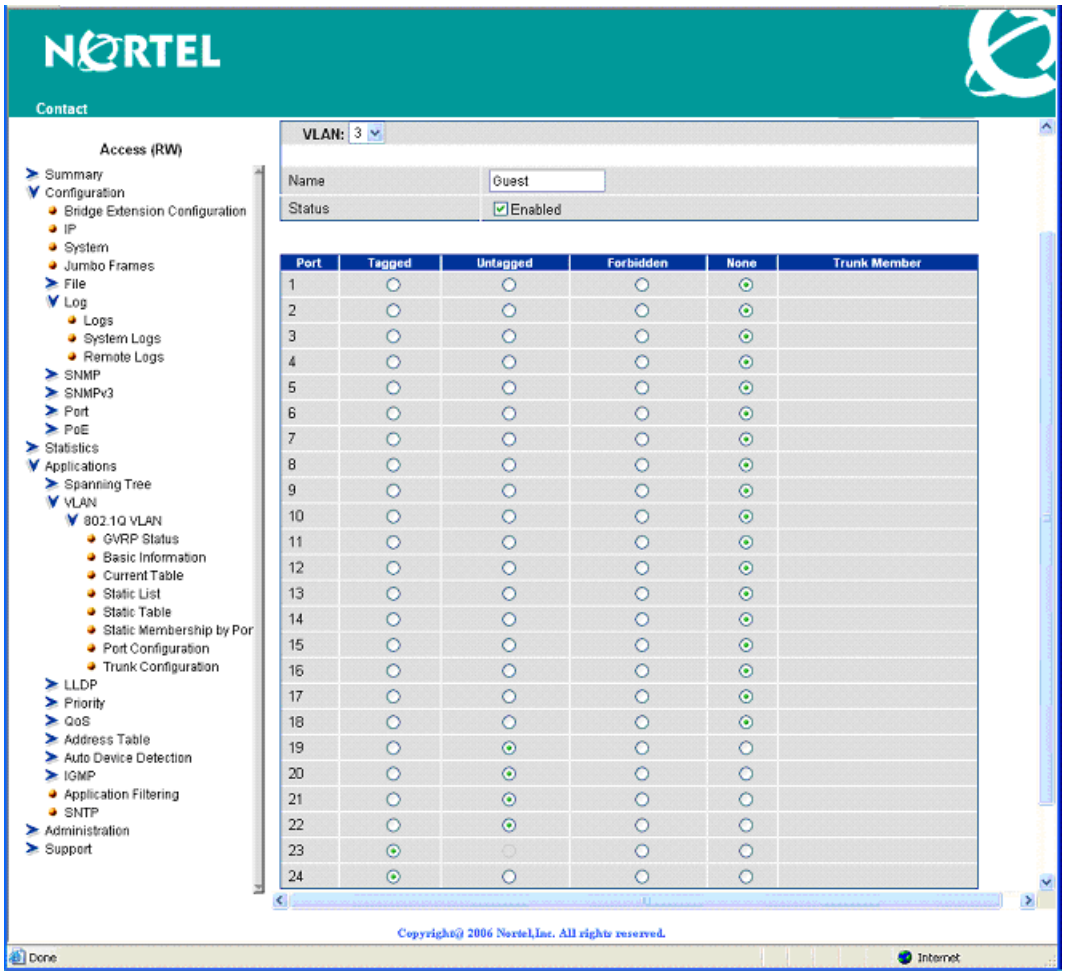
— For port 23 and 24, toggle the radio button under the Tagged column. This means port 23, 24 will be configured as a member of VLAN3 and egress frames will be tagged with VLAN ID 3.

— For port 19-22, toggle the radio button under the Untagged column. This means port 19-22 will be configured as a member of VLAN 3 and egress frames will be untagged.

— Click on the Submit button to apply the changes.

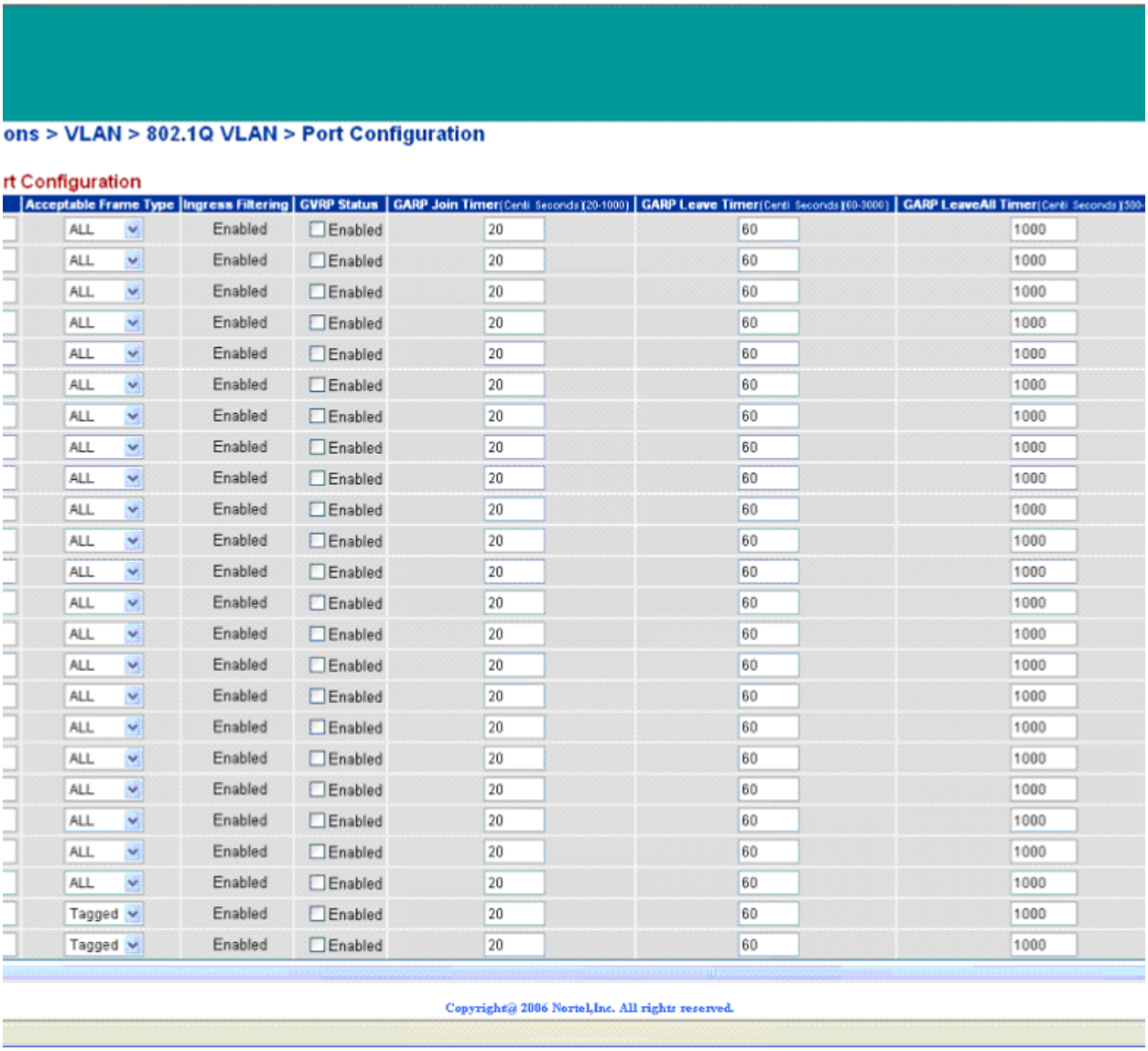
— A dialog box will pop up to advise the user that the PVID of the untagged member (in this case port 19-22) will automatically set to 2 (see the second and third screenshots).



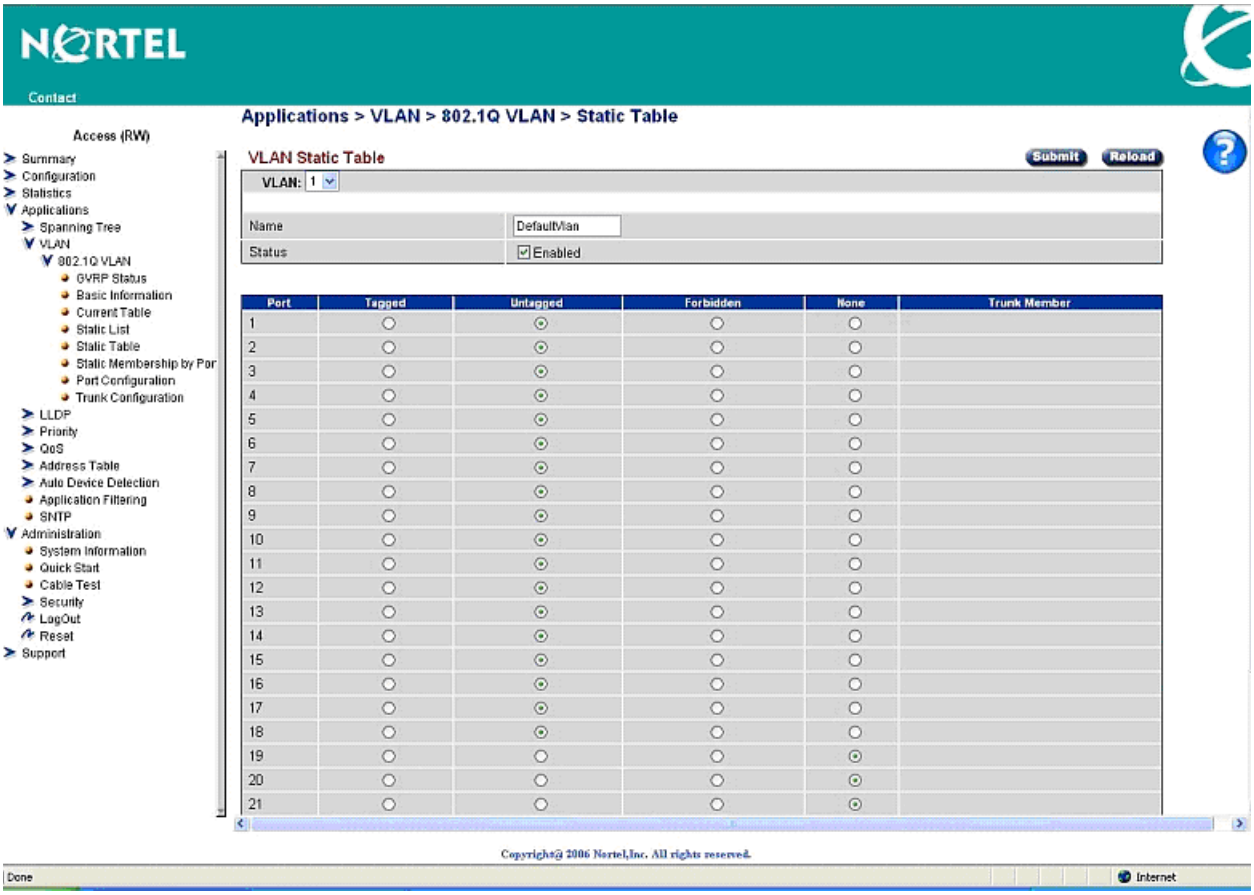

NORTEL
Contact
Access (RW)
Summary
Configuration
Bridge Extension Configuration
IP
System
Jumbo Frames
File
Log
Logs
System Logs
Remote Logs
SNMP
SNMPv3
Port
PoE
Statistics
Applications
Spanning Tree
VLAN
802.1Q VLAN
GVRP Status
Basic Information
Current Table
Static List
Static Table
Static Membership by Por
Port Configuration
Trunk Configuration
LLDP
Priority
QoS
Address Table
Auto Device Detection
IGMP
Application Filtering
SNTP
Administration
Support
VLAN: 3
Name
Guest
Status
Enabled
Port
Tagged
Untagged
Forbidden
None
Trunk Member
Copyright© 2006 Nortel,Inc. All rights reserved.
Done
Internet

Microsoft Internet Explorer
When join to untagged VLAN member, the Port's/Trunk's PVID will change to this VLAN.
OK

- Configure Port 23 and 24 as 802.1Q trunk port. Outgoing Ethernet frames are tagged with 802.1p/q tags, and incoming frames are tagged with appropriate 802.1p/q tags. Port 23 is used to connect to the BSG8ew via the GE port 8 on the BSG8ew and port 24 on the BES50 may be used for connecting to a second BES50 should it be needed.
  - From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Port Configuration to bring up the Port Configuration panel (see the first screenshot).
  - Under the VLAN Port Configuration section, change the Mode of port 23 and 24 from *Hybrid* to 1Q Trunk.
  - Change the Acceptable Frame Type of port 23 and 24 from *ALL* to *Tagged*.
  - Click on the Submit button to apply the changes.


ons > VLAN > 802.1Q VLAN > Port Configuration
rt Configuration
Acceptable Frame Type
Ingress Filtering
GVRP Status
GARP Join Timer(Centi Seconds)(20-1000)
GARP Leave Timer(Centi Seconds)(60-3000)
GARP LeaveAll Timer(Centi Seconds)(500-
ALL Enabled Enabled 20 60 1000
Tagged Enabled Enabled 20 60 1000
Copyright@ 2006 Nortel,Inc. All rights reserved.

- Rename VLAN 1 from “DefaultVlan” to “Data”.
- Configure Port 23 and 24 as “Tagged” member of VLAN1 (Data VLAN).
- Configure Port 13-18 as “Untagged” member of VLAN1 (Data VLAN).
- All other ports are not member of VLAN1 (Data VLAN).
  - — From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Static Table to bring up the Static Table panel. This panel manages the port membership of a specified VLAN, and the egress behavior of the membership ports.
  - — Under the VLAN Static Table section, select VLAN ID 1 from the VLAN drop down menu. Once VLAN 1 is selected, the panel will refresh to show the current port membership of VLAN 1. Note that the VLAN name of the default VLAN is *DefaultVlan* (see the first screenshot).
  - — From the Name entry box, change the VLAN name from *DefaultVlan* to *Data*.
  - — For port 23 and 24, toggle the radio button under the Tagged column. This means port 23, 24 will be configured as a member of VLAN1 and egress frames will be tagged with VLAN ID 1.
  - — Click on the Submit button to apply the changes.

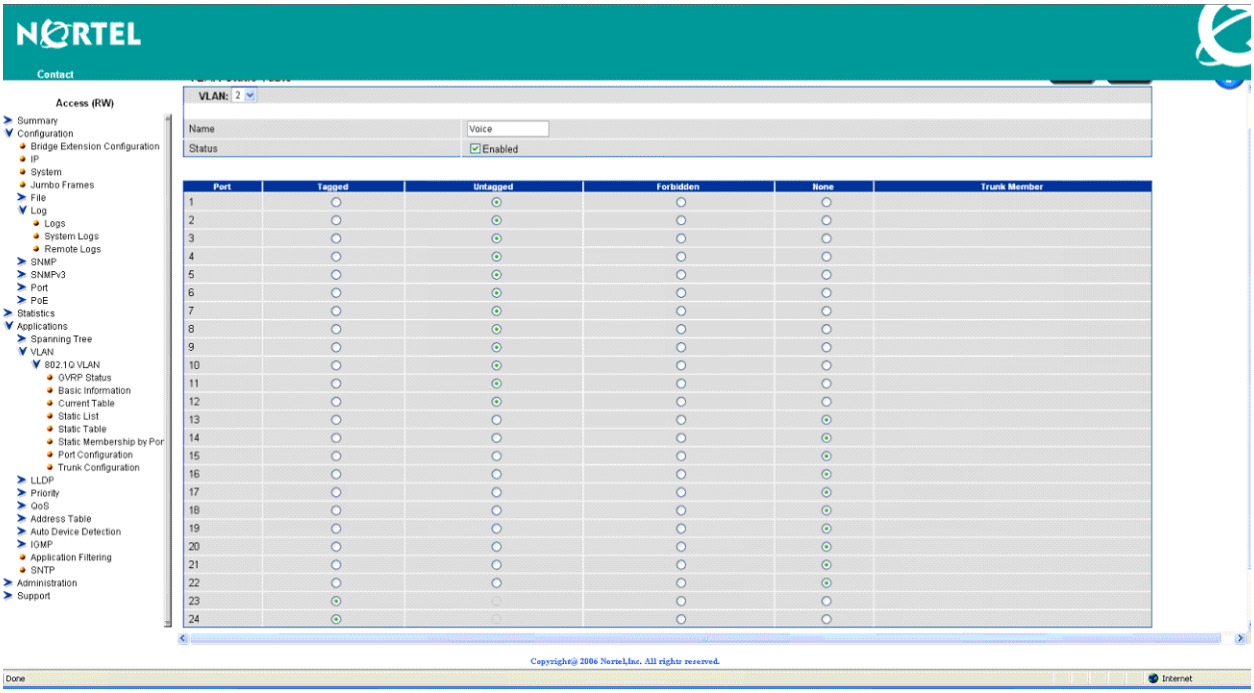


- Create new Voice VLAN 2.
  - From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Static List to bring up the Static List panel. This panel manages the VLAN currently configured on BES50. Under the VLAN Static List section, fill in the value *2* in the VLAN ID entry box.
  - Fill in the name *Voice* in the VLAN Name entry box.
  - Check the Status checkbox to enable the newly configured VLAN.
  - Click on the Add button to add the new VLAN to BES50.

- Configure Ports 1 to 12 inclusive as Untagged members of VLAN2 (Voice VLAN).
- Configure Port 23 and 24 as Tagged member of VLAN2 (Voice VLAN).
- All other ports are not member of VLAN2 (Guest VLAN).
  - From the left hand side menu tree, navigate to the item Applications > 802.1Q VLAN > Static Table to bring up the Static Table panel. This panel manages the port membership of a specified VLAN, and the egress behavior of the membership ports.
  - Under the VLAN Static Table section, select VLAN ID 3 from the VLAN drop down menu. Once VLAN 2 is selected, the panel will refresh to show the current port membership of VLAN 2. By default, none of the ports is member of a newly created VLAN.
  - For port 1-12, toggle the radio button under the Untagged column. This means port 1-12 will be configured as a member of VLAN3 and egress frames will be untagged.
  - For port 23 and 24, toggle the radio button under the Tagged column. This means port 23, 24 will be configured as a member of VLAN2 and egress frames will be tagged with VLAN ID 2.

— Click on the Submit button to apply the changes.

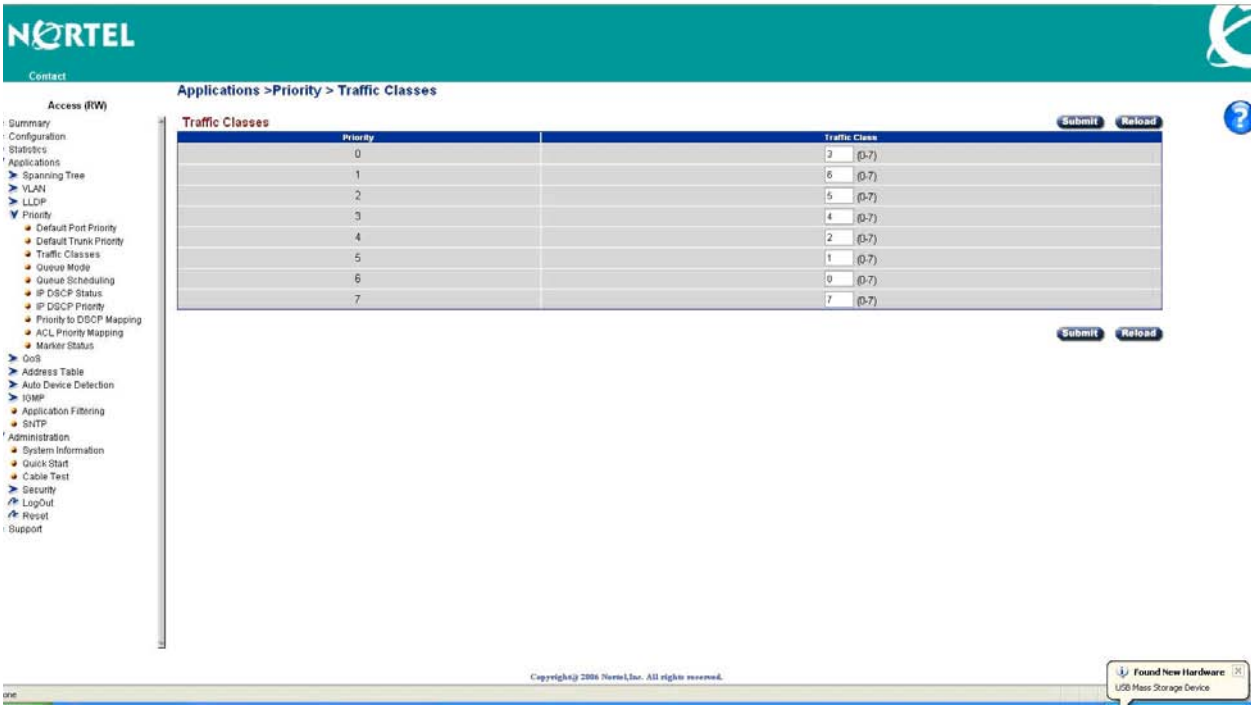
— A dialog box will pop up to advise the user that the PVID of the untagged member (in this case port 1-12) will automatically set to 2.



BES50 QoS configuration

- From the left hand side menu tree, navigate to the item Applications->Priority->Default Port Priority to bring up the Default Port Priority page. This page set the default 802.1p priority of the LAN ports. Untagged packets will have their priority set to the default priority configured for the ingress port.
  — Set the Default Port Priority of Ports 1 to 12 to 6
  — Set the Default Port Priority of Ports 13 to 18 to 5
  — Set the Default Port Priority of Ports 19 to 22 to 4
  — Click on the Submit button to apply the changes.
- From the left hand side menu tree, navigate to the item Applications->Priority->Traffic Classes to bring up the Traffic Classes Pages. This page is used to map 802.1p priority to one of the 8 egress queues.
  — Map priority 7 to Traffic Class 7
  — Map priority 6 to Traffic Class 0
  — Map priority 5 to Traffic Class 1
  — Map priority 4 to Traffic Class 2

— Map priority 3 to Traffic Class 4
— Map priority 2 to Traffic Class 5
— Map priority 1 to Traffic Class 6
— Map priority 0 to Traffic Class 3
— Click on the Submit button to apply the changes.



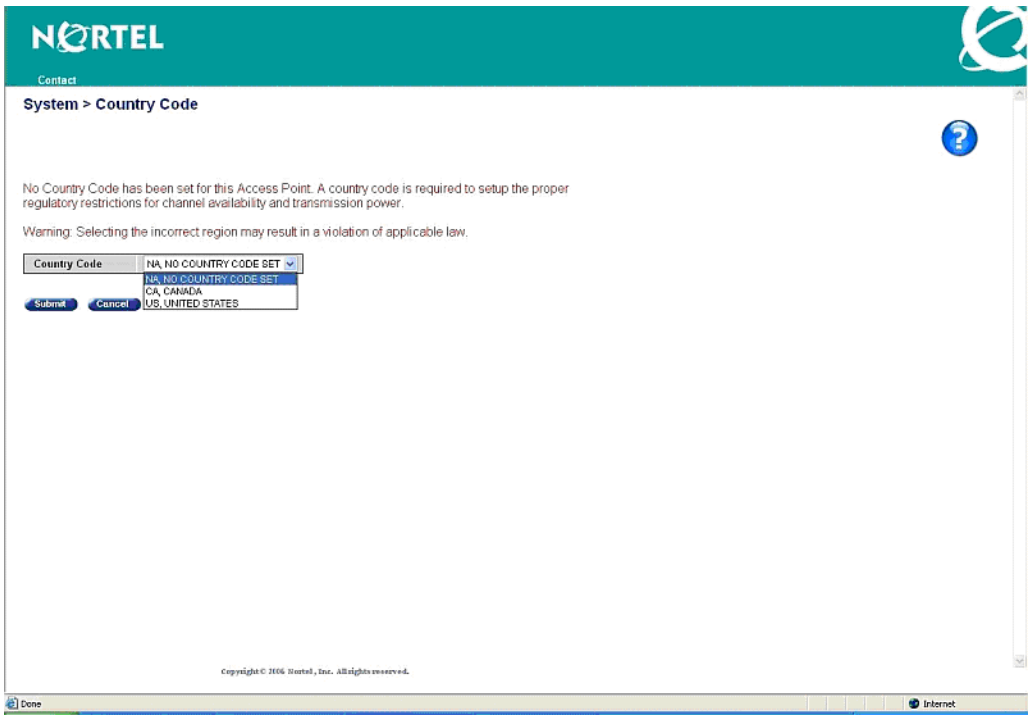
- From the left hand side menu tree, navigate to the item Applications->Priority->Queue Mode to bring up the Queue Mode page. From this page, the BES50 can be configured to use either Weighted Round Robin (WRR) or Strict Priority Scheduling. By default, the BES50 is configured to used WRR.
  — Change to Queue Mode to Strict and click on Submit to apply changes.

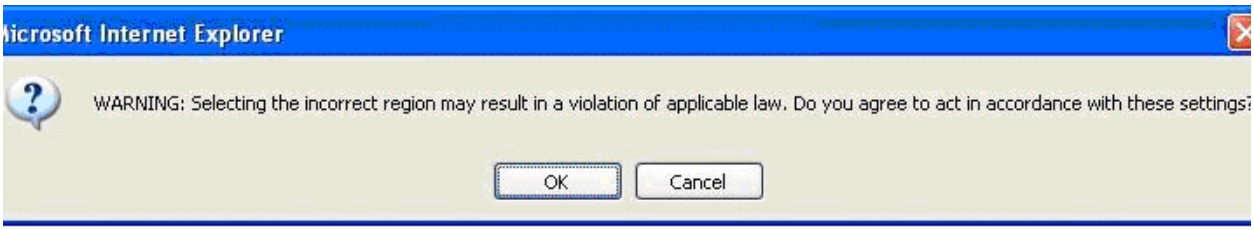
Pre-deployment configuration of BAP120-A

Country code configuration

- Configure the PC connected to the Ethernet port of the BAP120-A with an IP address of 192.168.1.1/24
- Launch your browser and point it to **http://192.168.1.136**

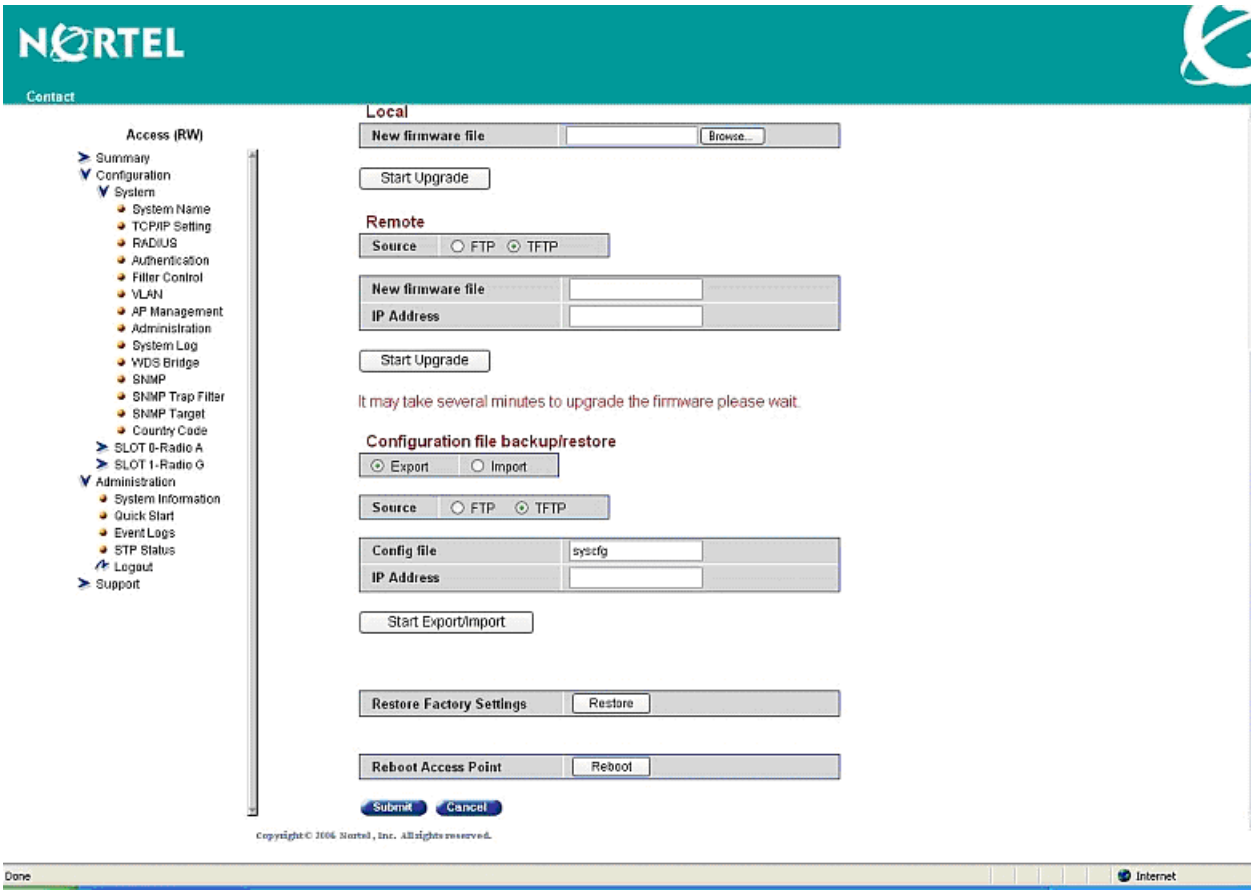
- Log onto the BAP120-A using the default username and password of *nnadmin* and *PlsChgMe!* respectively.
- Select the appropriate country code (either US or Canada).
  - By default, BAP120-A does not have any country code set. A country code panel will pop up the very first time BAP120-A is powered up and connected to (first screenshot).
  - NOTE: If BAP 120 has already been deployed with another country code, on the left hand side menu tree navigate to the item Configuration > System > Country Code to bring up the Country Code panel.
  - A warning dialog box will pop up to advise the user the importance of setting the correct country code (second screenshot).


NORTEL
Contact
System > Country Code
No Country Code has been set for this Access Point. A country code is required to setup the proper regulatory restrictions for channel availability and transmission power.
Warning: Selecting the incorrect region may result in a violation of applicable law.
Country Code
NA, NO COUNTRY CODE SET
NA, NO COUNTRY CODE SET
CA, CANADA
US, UNITED STATES
Submit
Cancel
Done
Internet


icrosoft Internet Explorer
WARNING: Selecting the incorrect region may result in a violation of applicable law. Do you agree to act in accordance with these settings?
OK
Cancel

- Reboot the access point to activate the selected country code.
  - From the left hand side menu tree, navigate to the item Configuration > System > Administration to bring up the Administration panel.

— Scroll to the bottom of the panel, and click on the Reboot button.

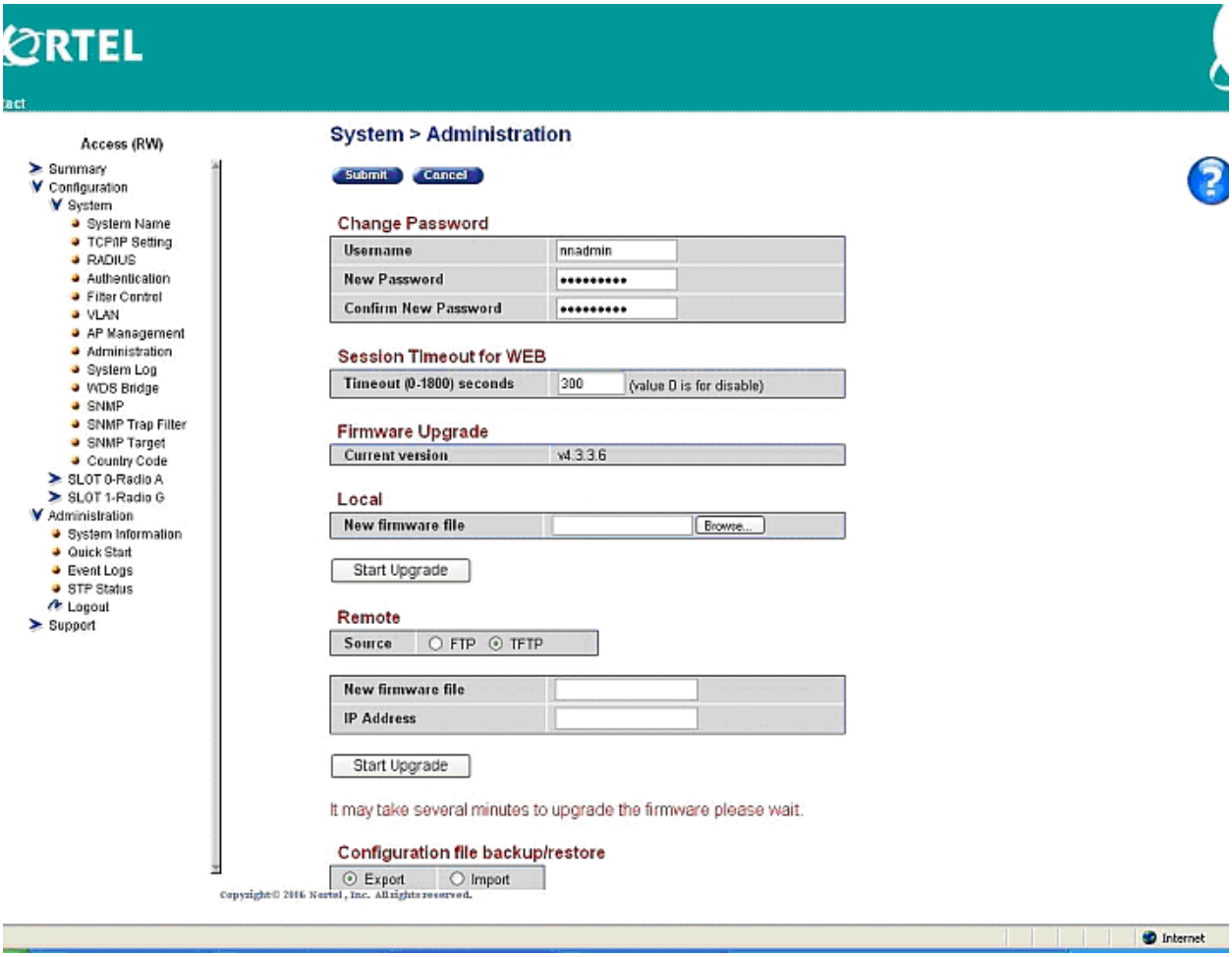


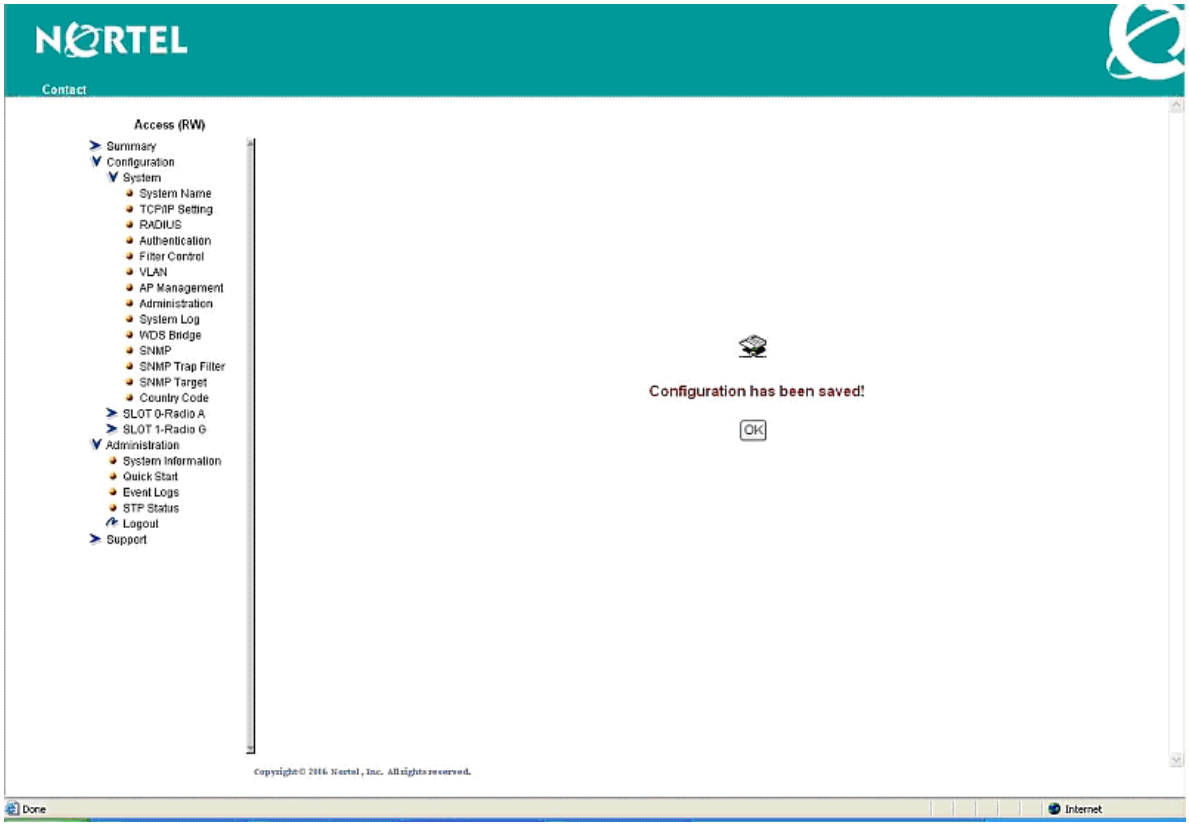
User management configuration

- Log onto the BAP120-A using the default username and password of *nnadmin* and *PlsChgMe!* respectively.
- Change the password of the default username.
- Change the WebUI timeout period from the default 60 seconds to 300 seconds.
  - — From the left hand side menu tree, navigate to the item Configuration > System > Administration to bring up the Administration panel.
  - — Under the Change Password section, type in the default username *nnadmin* in the UserName entry box.
  - — Type in the new password in the New Password entry box.
  - — Re-type the new password in the Confirm New Password entry box to ensure the password is correct.

— Under the Session Timeout for WEB section, type in the value of 300 seconds in the Timeout entry box.

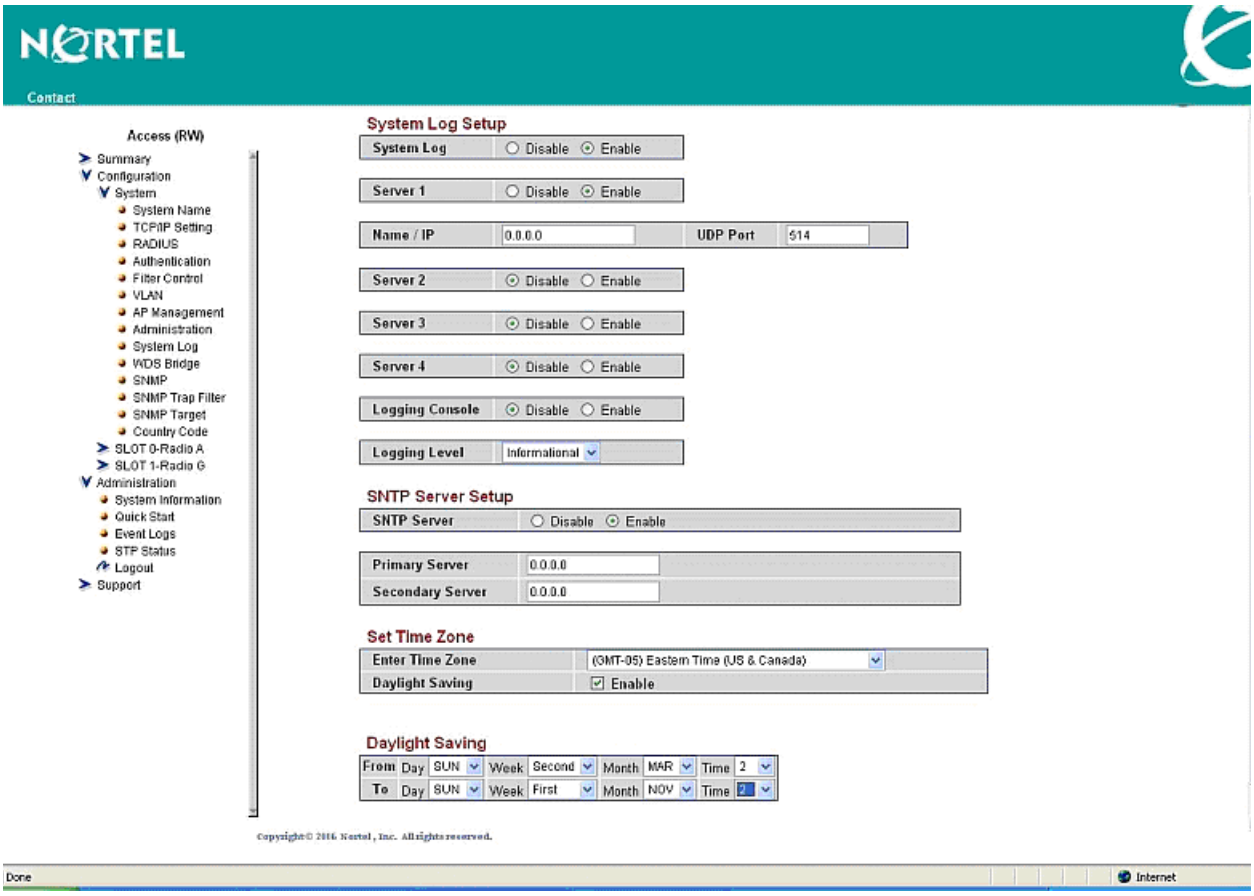
— Click on the Submit button to apply the changes.





Network management related OAM configuration

- Configure the BAP120-A to use the Syslog server located in the MSP network.
- Configure the BAP120-A to use the SNTP server located in the MSP network.
  - From the left hand side menu tree, navigate to the item Configuration > System > System Log to bring up the Syslog/SNTP panel.
  - Under the System Log Setup section, click on the radio button to enable System Log (syslog).
  - Click on the radio button to enable syslog Server 1.
  - Type in the syslog server IP address in the Server 1 IP entry box.
  - Under the SNTP Server Setup section, click on the radio button to enable SNTP Server.
  - Type in the SNTP server IP address in the Primary Server entry box.
  - Under the Set Time Zone section, from the drop down menu select the appropriate time zone where the BAP120-A is deployed. Click on the radio button to enable Daylight Saving if desired.
  - Under the Daylight Saving section, select appropriate daylight saving time period.
  - Click on the Submit button to apply the changes.



SSID configuration

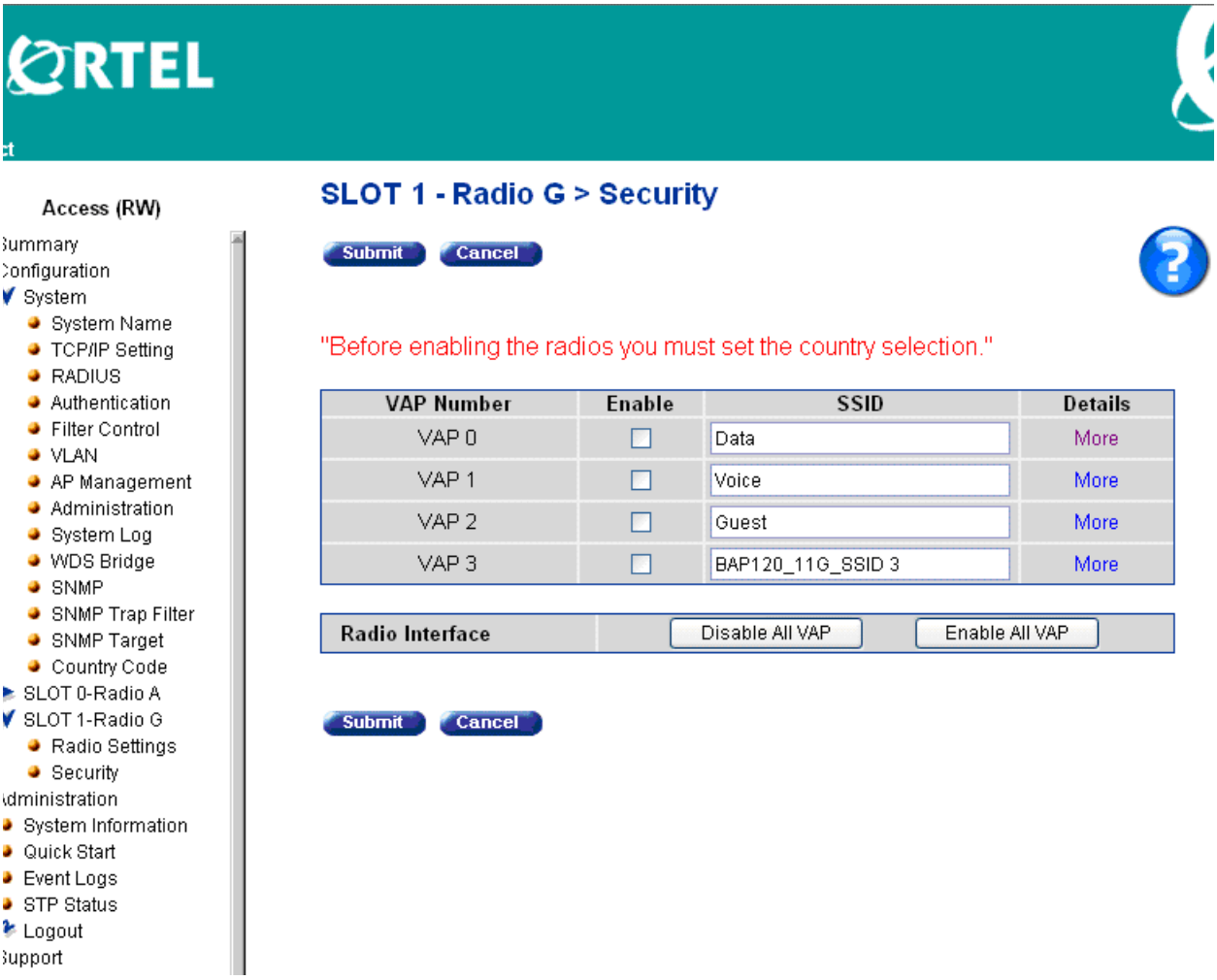
- By default, only the 802.11b/g radio is enabled and with only one SSID created for the access point. Create and configure three SSIDs to match the SSID and VLAN configuration for BSG8ew and BES50:

Table 28 – BAP120-A SSID to VLAN ID mapping

SSID	VLAN ID	Description
Data	1	Data SSID (Native vlan, Management and Data traffic)
Voice	2	Voice SSID
Guest	3	Guest SSID

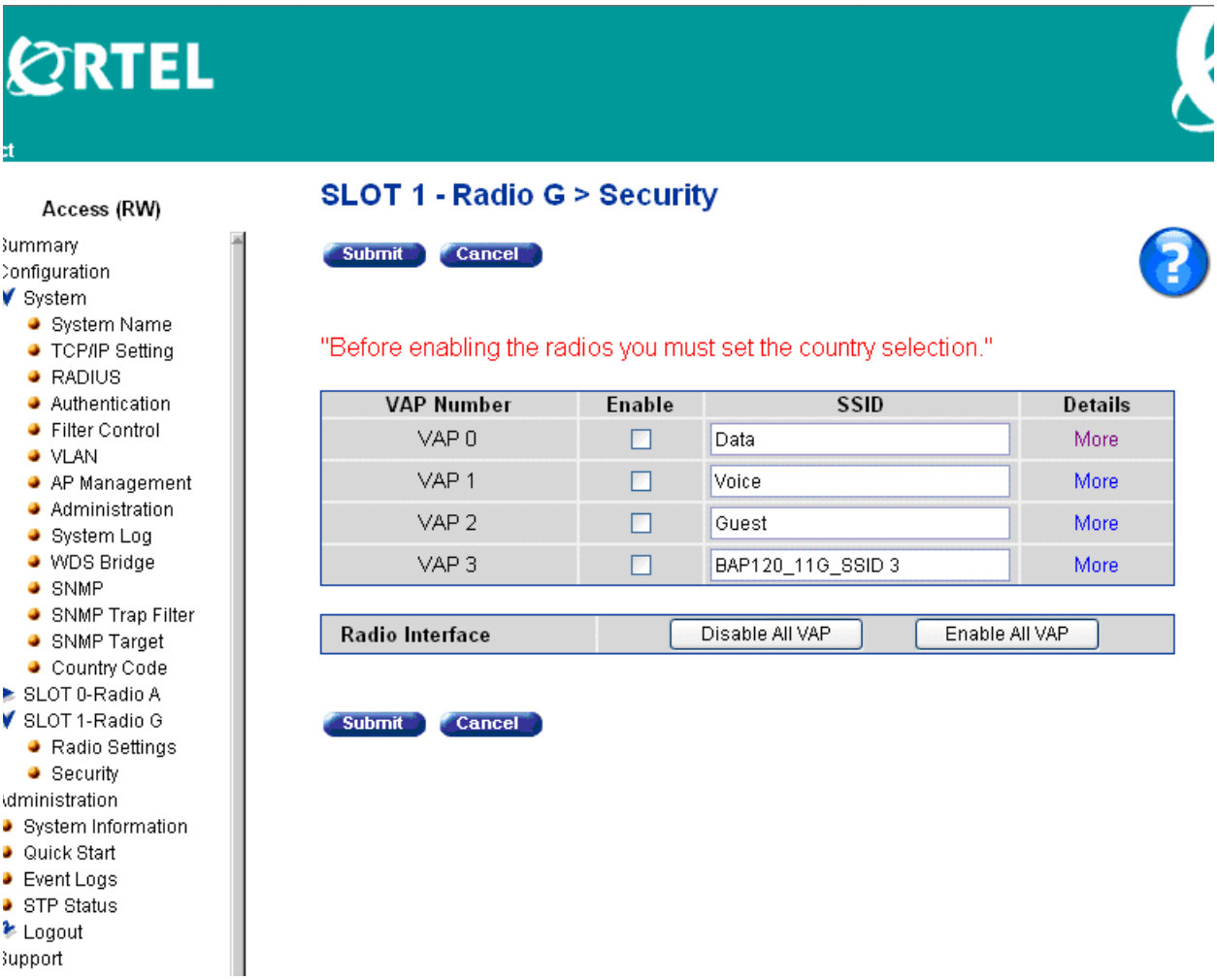
- Rename SSSID

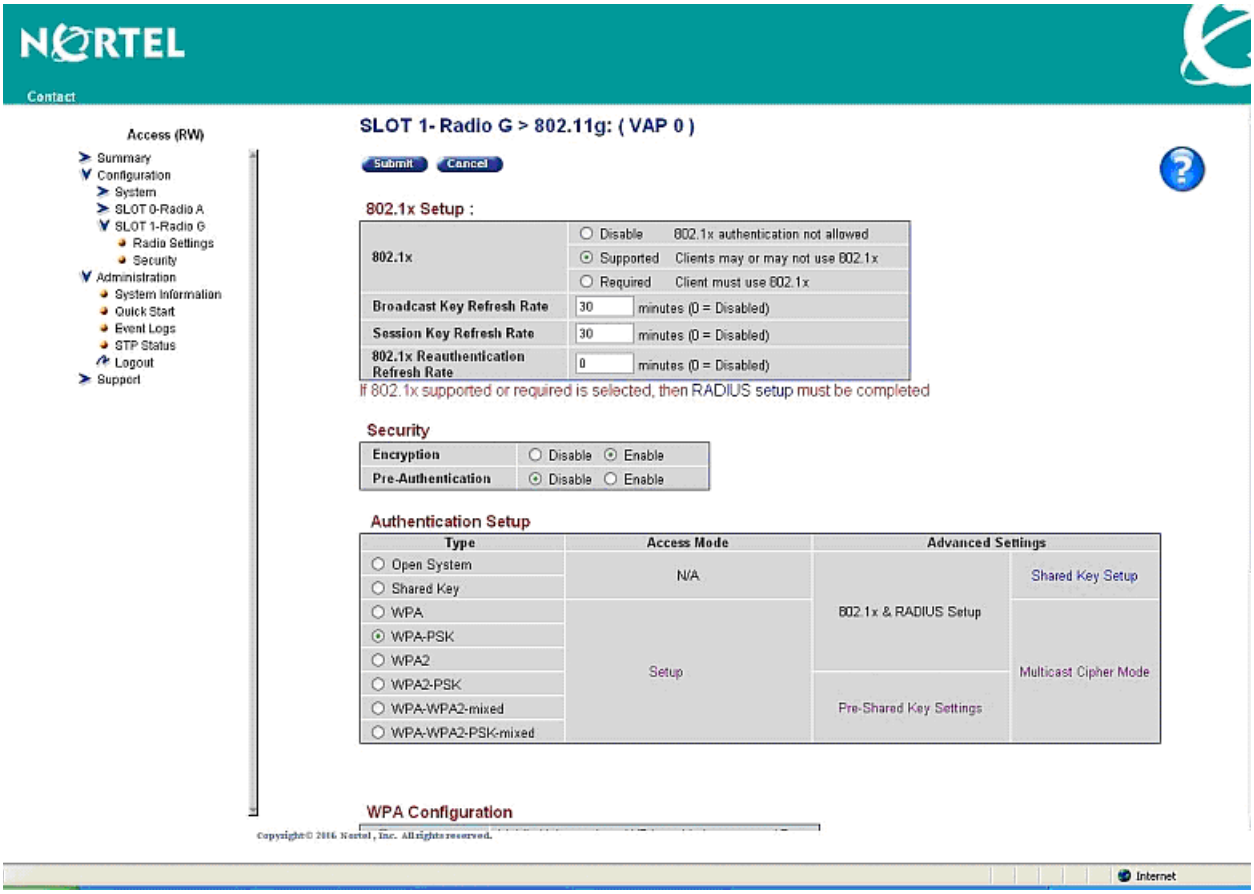
— Change the name of the first SSID (VAP 0) to “Data”.
— Change the name of the second SSID (VAP 1) to “Voice”.
— Change the name of the third SSID (VAP 2) to “Guest”
— Disable all SSIDs before configuration is completed.
    - From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Security to bring up the VAP/SSID panel.
    - Change the VAP 0 SSID name from the default value of *BAP120_11G_SSID 0* to *Data*.
    - Change the VAP 1 SSID name from the default value of *BAP120_11G_SSID 1* to *Voice*
    - Change the VAP 2 SSID name from the default value of *BAP120_11G_SSID 2* to *Guest*..
    - Click on the Disable All VAP button to disable all the SSID/VAP.
    - Click on the Submit button to apply the changes.

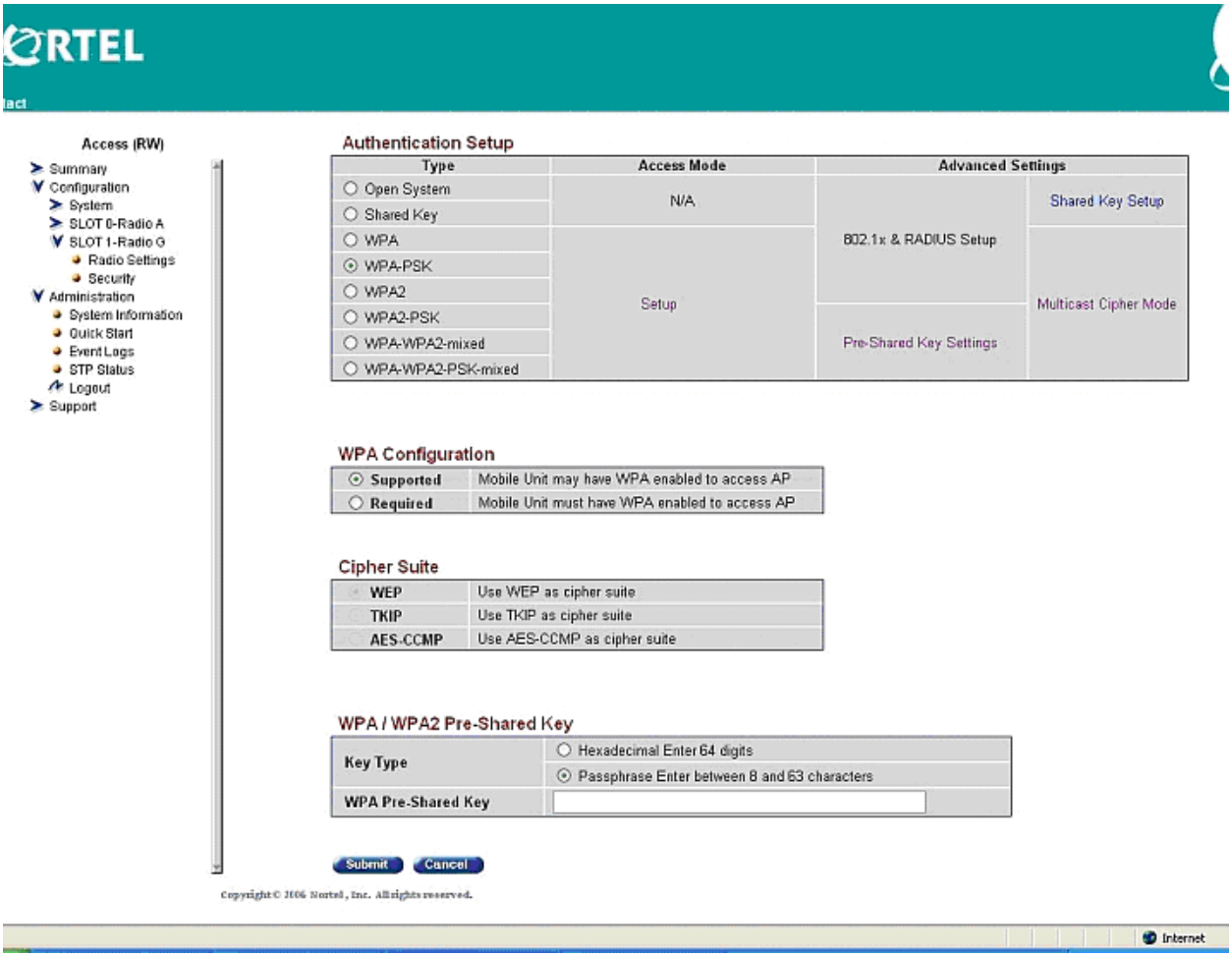


- Modify SSID 1 (Data) as follows:
  - Enable WPA-PSK
  - Configure the pre-shared key. Make sure this is the same value as the configured on the BSG8ew.
    - From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Security to bring up the VAP/SSID panel (first screenshot).
    - Click on the link labeled More on VAP0 with SSID name *Data* to bring up the Security panel for the *Data* SSID (second and third screenshot).
    - Under the 802.1x Setup section, click on the radio button labeled Supported to enable 802.1x support on the Data SSID.
    - Under the Security section, click on the radio button to enable Encryption.
    - Under the Authentication Setup section, click on the radio button to select WPA-PSK authentication.

- Under the WPA Configuration section, click on the radio labeled Supported to enable WPA support on the *Data* SSID.
- Under the WPA/WPA2 Pre-Shared Key section, click on the radio button to select ASCII Passphase Key Type.
- Type in a 8-63 characters ASCII pre-shared key in the WPA Pre-Shared Key entry box. Make sure this pre-shared key is the same as that configured on BSG8ew.
- Click on the Submit button to apply the changes.


RTEL
Access (RW)
Summary
Configuration
System
System Name
TCP/IP Setting
RADIUS
Authentication
Filter Control
VLAN
AP Management
Administration
System Log
WDS Bridge
SNMP
SNMP Trap Filter
SNMP Target
Country Code
SLOT 0-Radio A
SLOT 1-Radio G
Radio Settings
Security
Administration
System Information
Quick Start
Event Logs
STP Status
Logout
Support
SLOT 1 - Radio G > Security
Submit
Cancel
"Before enabling the radios you must set the country selection."
VAP Number
Enable
SSID
Details
VAP 0
Data
More
VAP 1
Voice
More
VAP 2
Guest
More
VAP 3
BAP120_11G_SSID 3
More
Radio Interface
Disable All VAP
Enable All VAP
Submit
Cancel


NORTEL
Contact
Access (RW)
Summary
Configuration
System
SLOT 0-Radio A
SLOT 1-Radio G
Radio Settings
Security
Administration
System Information
Quick Start
Event Logs
STP Status
Logout
Support
SLOT 1- Radio G > 802.11g: (VAP 0)
Submit
Cancel
802.1x Setup :
802.1x
Disable 802.1x authentication not allowed
Supported Clients may or may not use 802.1x
Required Client must use 802.1x
Broadcast Key Refresh Rate
30 minutes (0 = Disabled)
Session Key Refresh Rate
30 minutes (0 = Disabled)
802.1x Reauthentication Refresh Rate
0 minutes (0 = Disabled)
If 802.1x supported or required is selected, then RADIUS setup must be completed
Security
Encryption
Disable Enable
Pre-Authentication
Disable Enable
Authentication Setup
Type
Access Mode
Advanced Settings
Open System
Shared Key
N/A
Shared Key Setup
WPA
WPA-PSK
WPA2
WPA2-PSK
WPA-WPA2-mixed
WPA-WPA2-PSK-mixed
Setup
802.1x & RADIUS Setup
Pre-Shared Key Settings
Multicast Cipher Mode
WPA Configuration
Internet

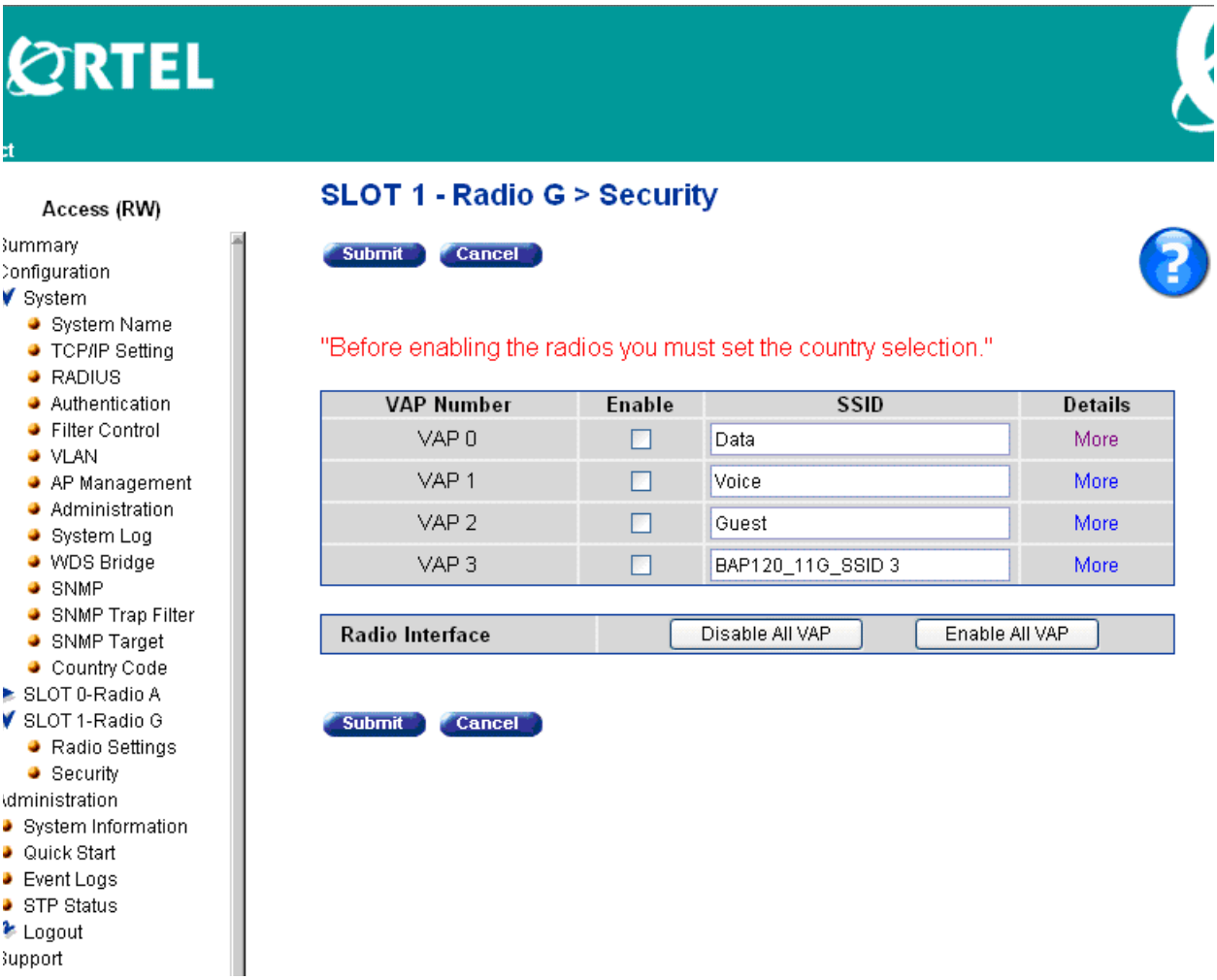


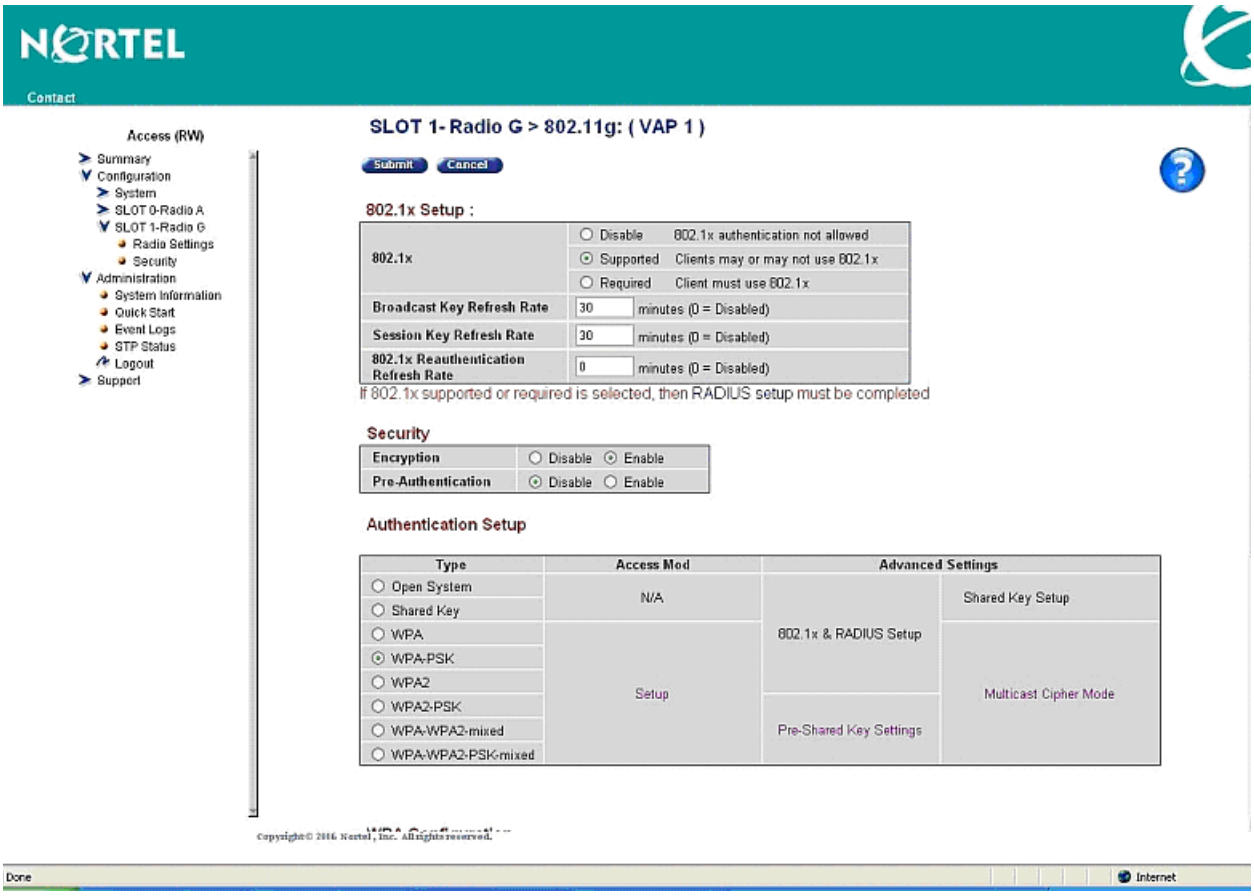
- Modify SSID 2 (Voice) as follows:
  - Enable WPA-PSK
  - Configure the pre-shared key, and ensure the pre-shared key is the same as that configured for the Guest SSID on the BSG8ew.
  - From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Security to bring up the VAP/SSID panel (first screenshot).
  - Click on the link labeled More on VAP1 with SSID name *Voice* to bring up the Security panel for the *Voice* SSID (second and third screenshot).
  - Under the 802.1x Setup section, click on the radio button labeled Supported to enable 802.1x support on the *Voice* SSID.
  - Under the Security section, click on the radio button to enable Encryption.
  - Under the Authentication Setup section, click on the radio button to select WPA-PSK authentication.
  - Under the WPA Configuration section, click on the radio labeled Supported to enable WPA support on the *Voice* SSID.

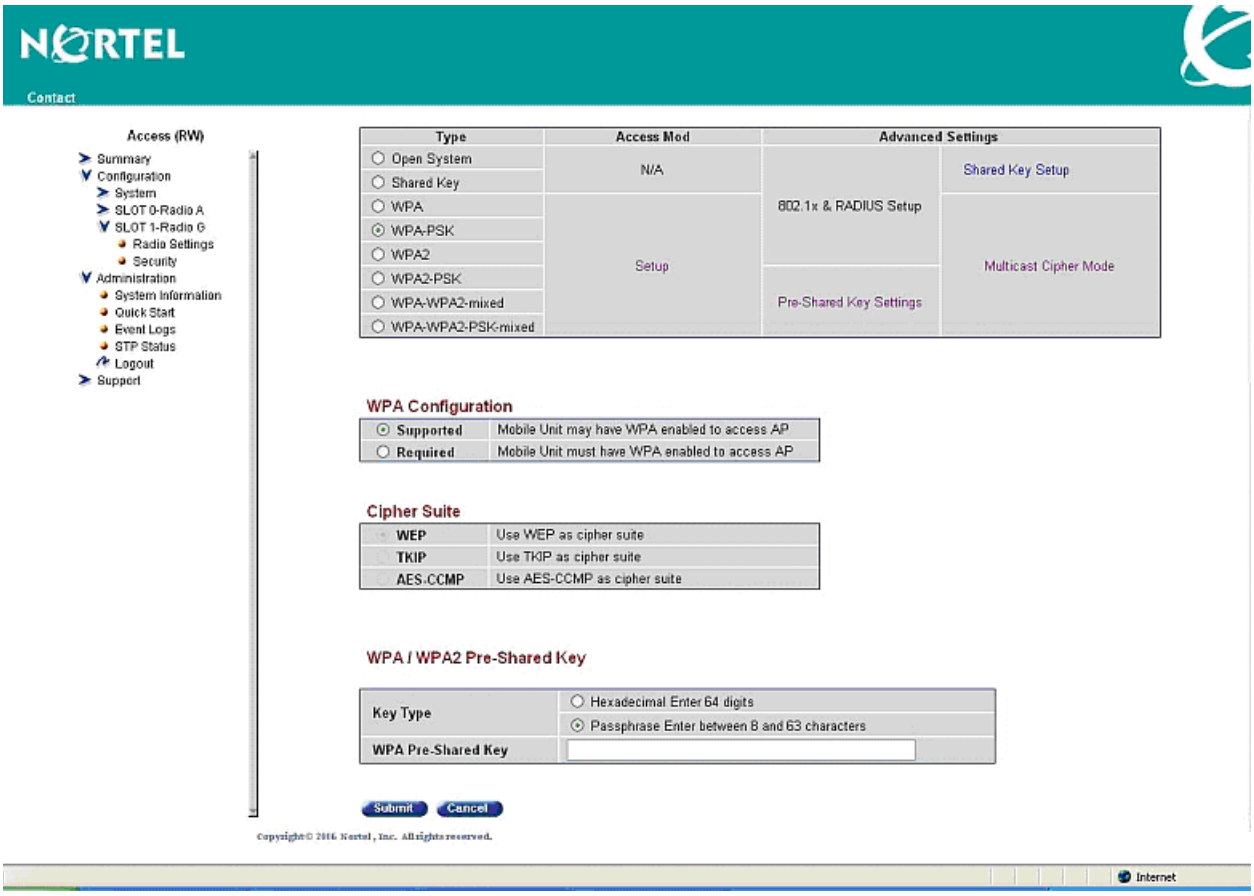
— Under the WPA/WPA2 Pre-Shared Key section, click on the radio button to select ASCII Passphase Key Type.

— Type in a 8-63 characters ASCII pre-shared key in the WPA Pre-Shared Key entry box. Again, this key should be the same as that configured for Voice SSID on BSG8ew.

— Click on the Submit button to apply the changes.

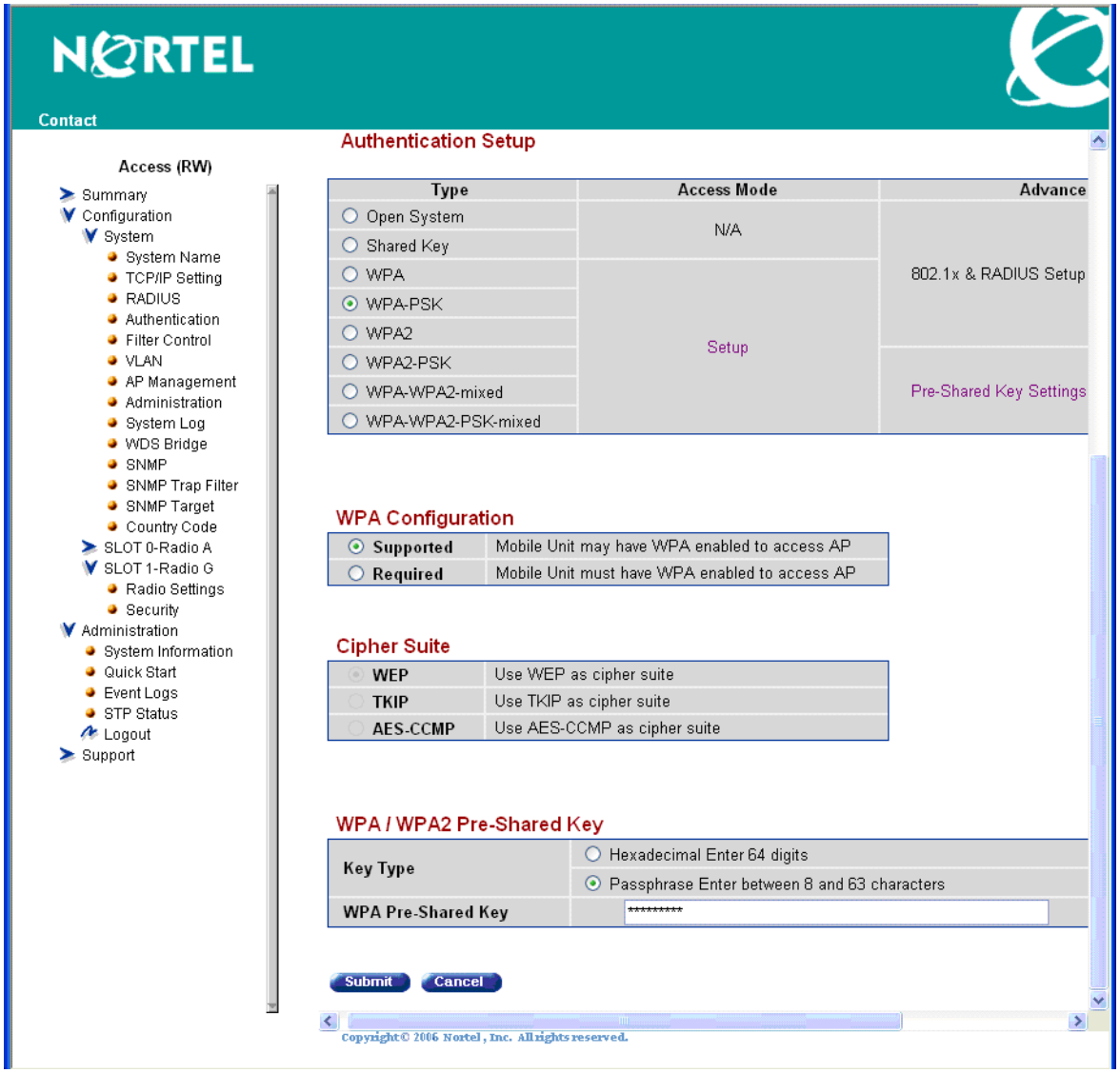



NORTEL
Contact
Access (RW)
Summary
Configuration
System
SLOT 0-Radio A
SLOT 1-Radio G
Radio Settings
Security
Administration
System Information
Quick Start
Event Logs
STP Status
Logout
Support
SLOT 1- Radio G > 802.11g: (VAP 1)
Submit
Cancel
802.1x Setup :
802.1x
Disable 802.1x authentication not allowed
Supported Clients may or may not use 802.1x
Required Client must use 802.1x
Broadcast Key Refresh Rate
30 minutes (0 = Disabled)
Session Key Refresh Rate
30 minutes (0 = Disabled)
802.1x Reauthentication Refresh Rate
0 minutes (0 = Disabled)
If 802.1x supported or required is selected, then RADIUS setup must be completed
Security
Encryption
Disable Enable
Pre-Authentication
Disable Enable
Authentication Setup
Type
Access Mod
Advanced Settings
Open System
Shared Key
N/A
802.1x & RADIUS Setup
Shared Key Setup
WPA
WPA-PSK
WPA2
WPA2-PSK
WPA-WPA2-mixed
WPA-WPA2-PSK-mixed
Setup
Multicast Cipher Mode
Pre-Shared Key Settings
Copyright© 2006 Nortel, Inc. All rights reserved.
Done
Internet



- Modify SSID 3 (Guest) as follows:
  - — Enable WPA-PSK
  - — Configure the pre-shared key. Make sure this is the same value as the configured on the BSG8ew.
    - From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Security to bring up the VAP/SSID panel.
    - Click on the link labeled More on VAP2 with SSID name *Guest* to bring up the Security panel for the *Guest* SSID.
    - Under the 802.1x Setup section, click on the radio button labeled Supported to enable 802.1x support on the *Guest* SSID.
    - Under the Security section, click on the radio button to enable Encryption.
    - Under the Authentication Setup section, click on the radio button to select WPA-PSK authentication.

- Under the WPA Configuration section, click on the radio labeled Supported to enable WPA support on the *Guest* SSID.
- Under the WPA/WPA2 Pre-Shared Key section, click on the radio button to select ASCII Passphase Key Type.
- Type in a 8-63 characters ASCII pre-shared key in the WPA Pre-Shared Key entry box. Again, this key should be the same as that configured for Guest SSID on BSG8ew.
- Click on the Submit button to apply the changes.



SSID to VLAN mapping

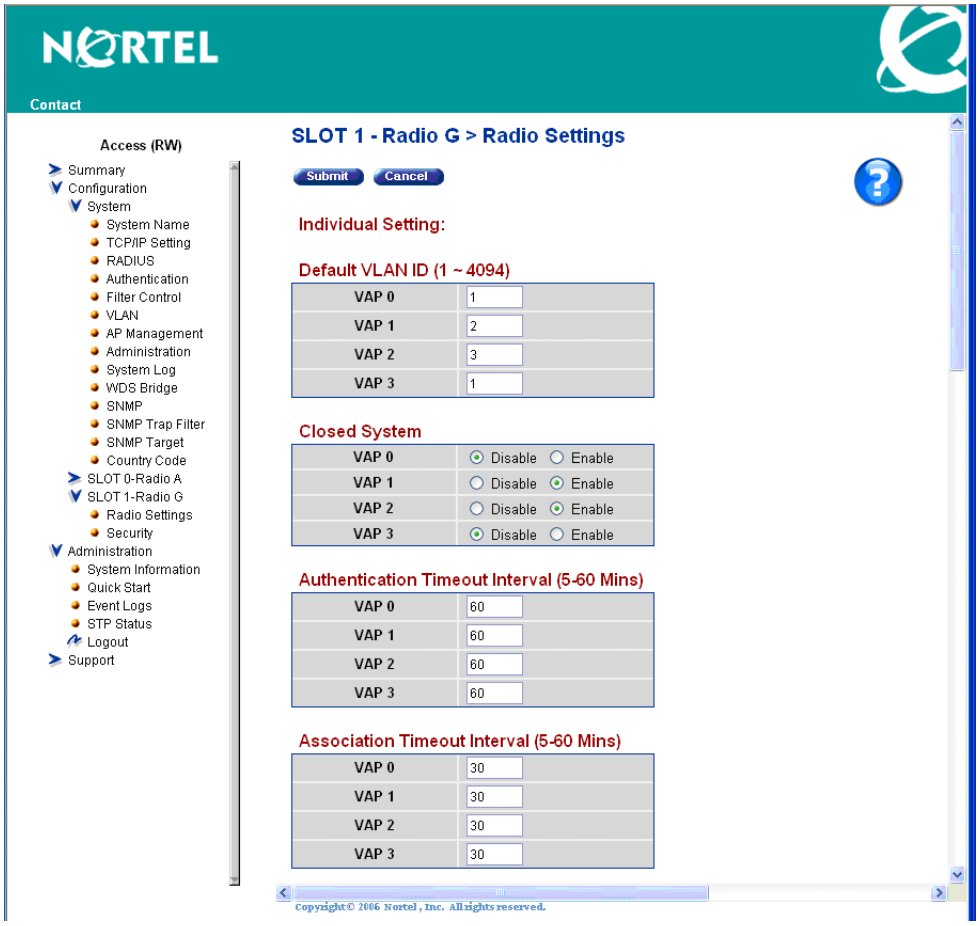
- By default, SSID broadcast is enabled for all the configured SSID (or VAP).
- Disable SSID broadcast (i.e. enable Closed System) for the Data SSID (VAP 0).
- Map Data SSID (VAP 0) to the VLAN ID 1 for the Data VLAN (see Table 28 – BAP120-A SSID to VLAN ID mapping).
- Map Voice SSID (VAP 1) to the VLAN ID 2 for the Voice VLAN (see Table 28 – BAP120-A SSID to VLAN ID mapping)
- Map Guest SSID (VAP 2) to the VLAN ID 3 for the Guest VLAN (see Table 28 – BAP120-A SSID to VLAN ID mapping)

— From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Radio Settings to bring up the radio setting panel.

— Under the Default VLAN ID section, type in the value 1 in the VAP0 entry box (corresponding to the *Data* SSID); type in the value 2 in the VAP1 entry box (corresponding to the *Guest* SSID).

— Under the Closed System section, click on the radio button to enable closed system feature (i.e. disable SSID Broadcast) for VAP0 (corresponding to the *Data* SSID).

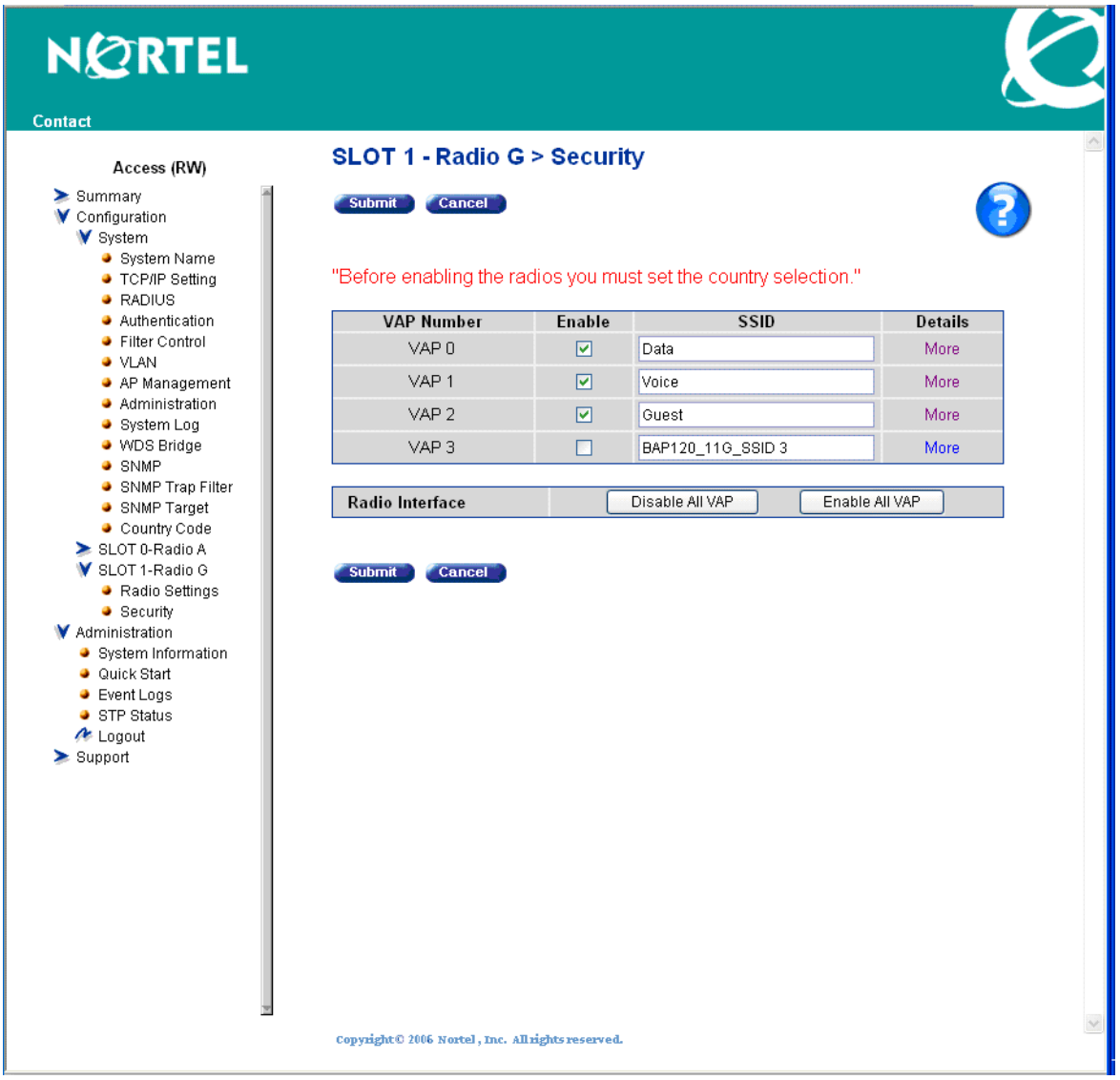
— Click on the Submit button to apply the changes.



Enable SSID

- Enable all three SSIDs: Data, Voice and Guest
  — From the left hand side menu tree, navigate to the item Configuration > SLOT 1-Radio G > Security to bring up the VAP/SSID panel.
  — Check the checkbox corresponding to VAP0 with SSID name *Data* to enable the SSID.
  — Check the checkbox corresponding to VAP1 with SSID name *Voice* to enable the SSID.

— Check the checkbox corresponding to VAP2 with SSID name Guest to enable the SSID
— Uncheck the checkbox corresponding to VAP3 to disable this SSID.
— Click on the Submit button to apply the changes.



Enable VLAN

- By default, VLAN support is disabled on BAP120-A. The very last step is to enable VLAN support on BAP120-A. NOTE: This must be the last step, otherwise the WebUI may not be able to connect to the BAP120-A unless both
  — From the left hand side menu tree, navigate to the item Configuration > System VLAN to bring up the VLAN configuration panel.

— Under the VLAN Configuration section, click on the radio button to enable VLAN Classification. This effectively turns the Ethernet port into 802.1Q trunk port and expecting ingress frame into the Ethernet port are all properly tagged.

NOTE that the default VLAN ID for the management of BAP120-A is VLAN 1.

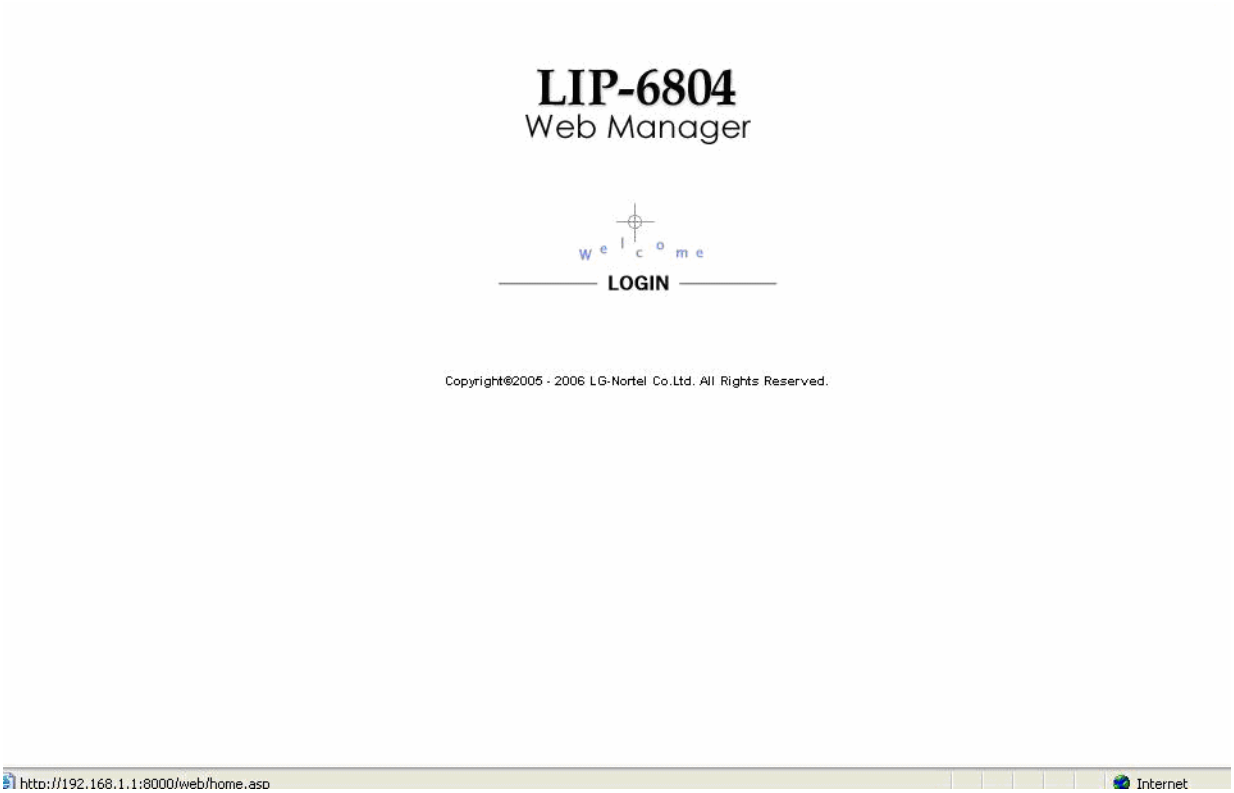
— Click on the Submit button to apply the changes.

— A warning dialog will pop up to advise the user that the BAP120-A access point must now connected to a 802.1Q trunk port which must be at least a member of VLAN1.

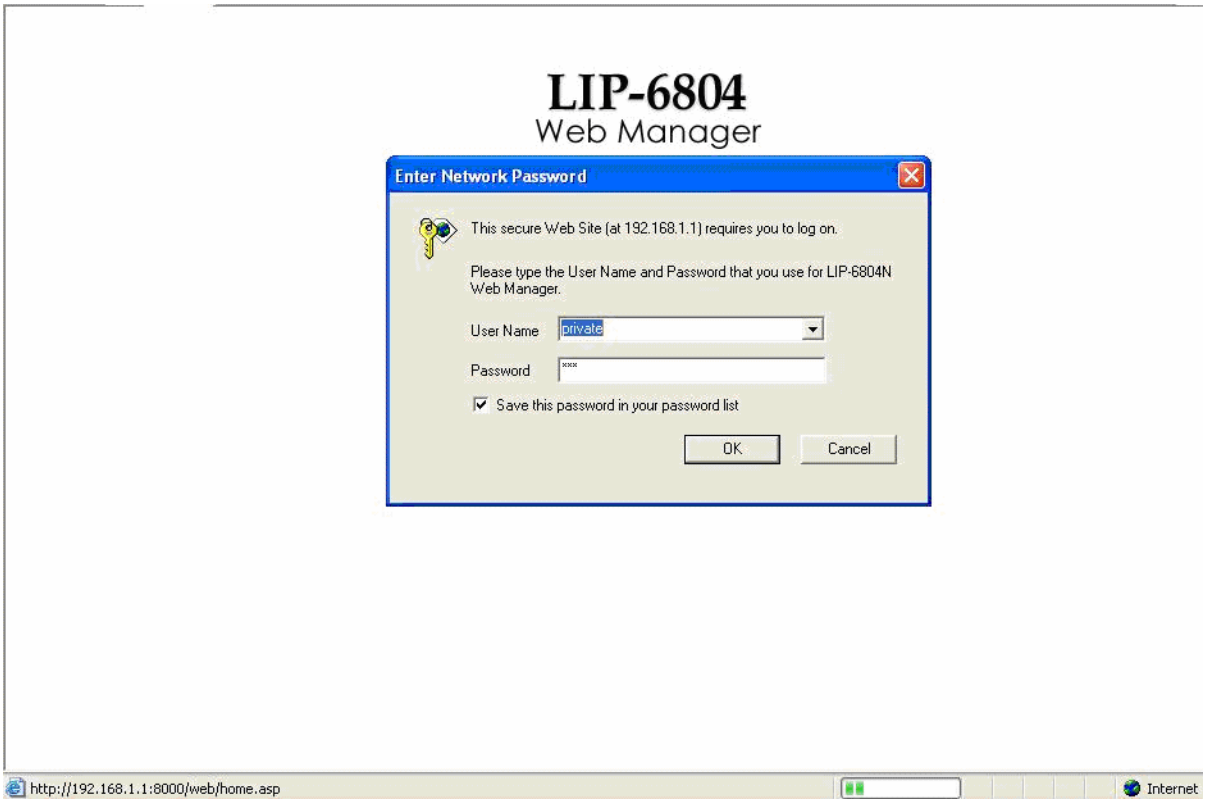
Pre-deployment configuration of LG6800 series phones

This section describes the procedures for configuring the LG-Nortel 6800 series of phones for use with the BSG8ew. These configurations must be done prior to installing the phone at the customer premises.

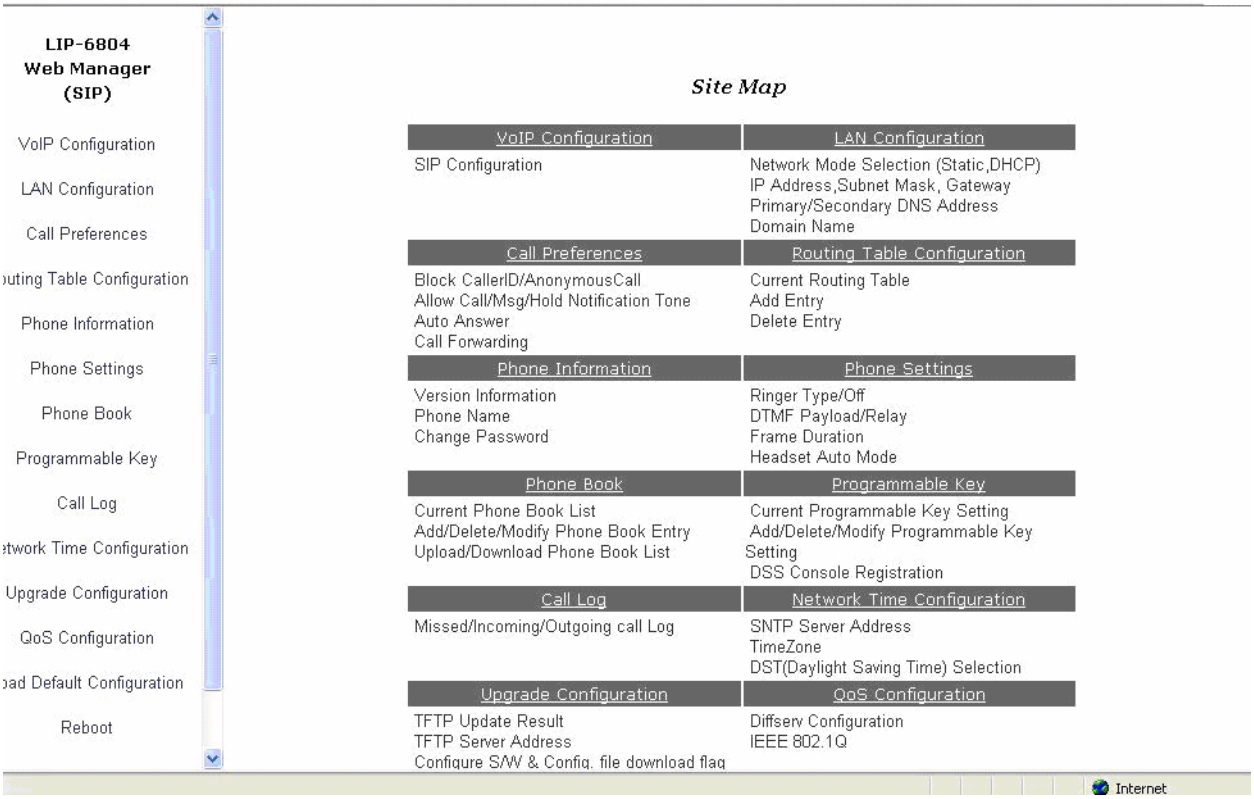
- Configure the NIC card of a PC with an IP address of 192.168.1.254.
- Connect one end of an Ethernet cable to the PC and the other end to the Ethernet port under the LG-Nortel phone. Make sure to connect the cable into the port labeled LAN.
- Power on the LG-Nortel phone and wait for about 3 minutes.
- From your PC, launch a web browser and point it to **http://192.168.1.1:8000**
- The LG-Nortel Web Manager page will be displayed.
- To log into the phone, click on the Welcome sign as shown in the figure below:



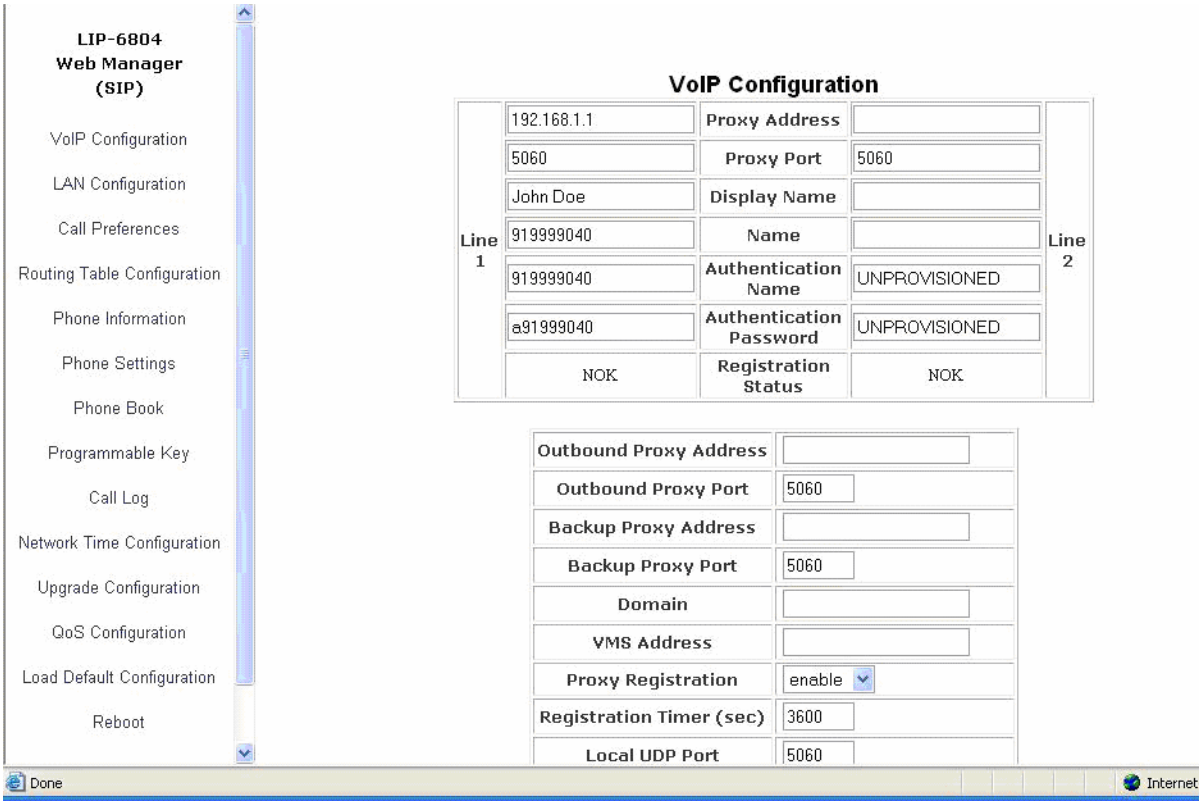
- When the login window pops up, login into the phone with user name of *private* and password *lip* and click OK.



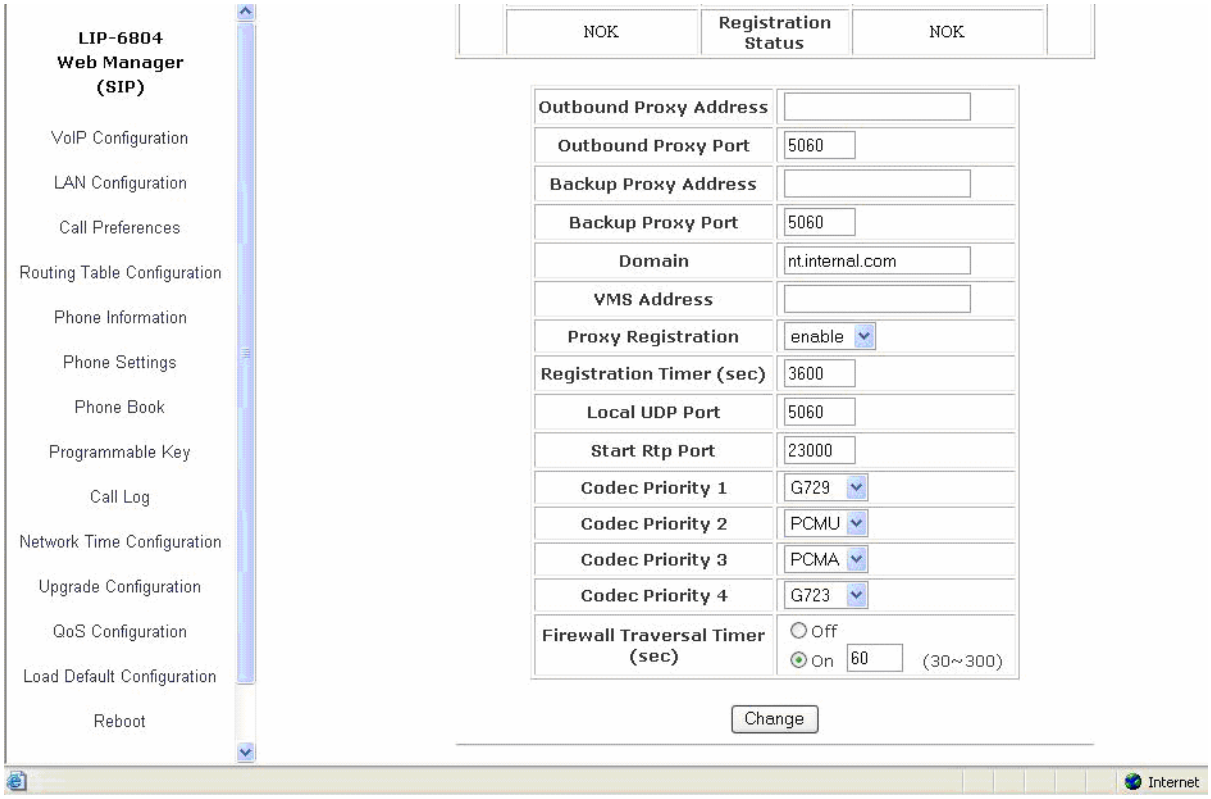
- On the Site MAP page, click on **VoIP Configuration** to configure the phone for SIP.



- In the VoIP Configuration page, configure **Line 1** of the phone with the following:
- **Proxy Address** set to 192.168.1.1
- **Display Name** set to name of the user that will be using this phone for example John Doe. This will be the name that is displayed as the callee.
- **Name** set to username for the account. This should be the same as that configured on the CS2K.
- Set the **Authentication Name** to the value defined on the CS2K. This is that name that will be authenticated by the SIP server.
- Set the **Authentication Password** to the password defined on the CSK for the above Authentication Name. The phone will provide this password when challenged by the CS2K during registration. Make sure this value matches what is defined on the CS2K.



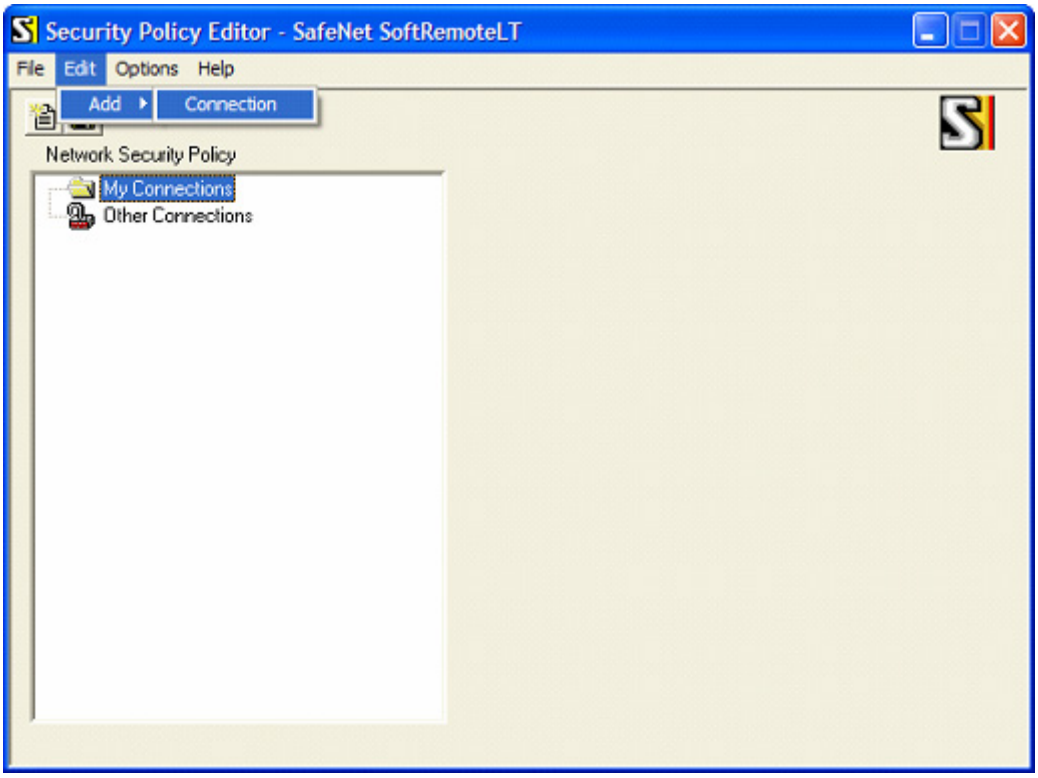
- Configure the LG-Nortel Phone with Home Domain of the CS2K SIP server. This must be the same as that configured on the BSG8ew and on the CS2K. On the phone, this is done by setting to the **Domain** field to the Home Domain. In this example, the domain is set to nt.internal.com
- Change the **Codec Priority 2** from G723 to PCMU
- Change the **Codec Priority 3** from PCMU to PCMA
- Change the **Codec Priority 4** from PCMA to G723
- Click on the **Change** button at the bottom of the page to save and apply your changes.



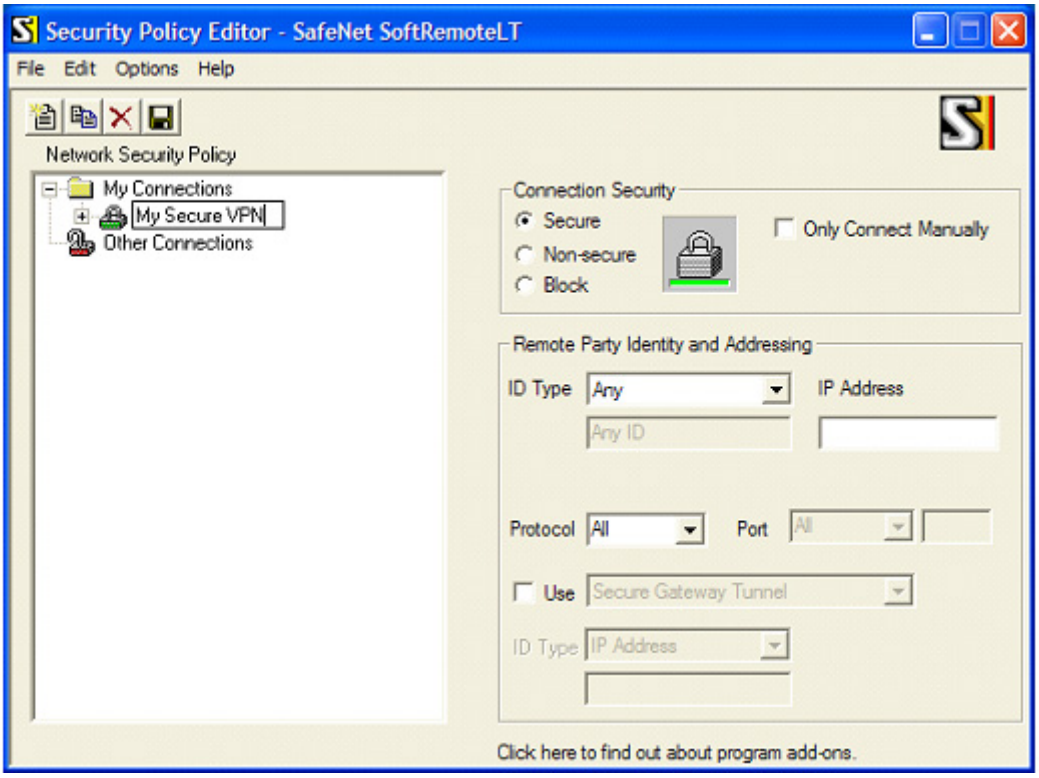
- Click on Reboot on the left hand navigation panel for changes to take effect.

Pre-deployment configuration of SafeNet VPN client

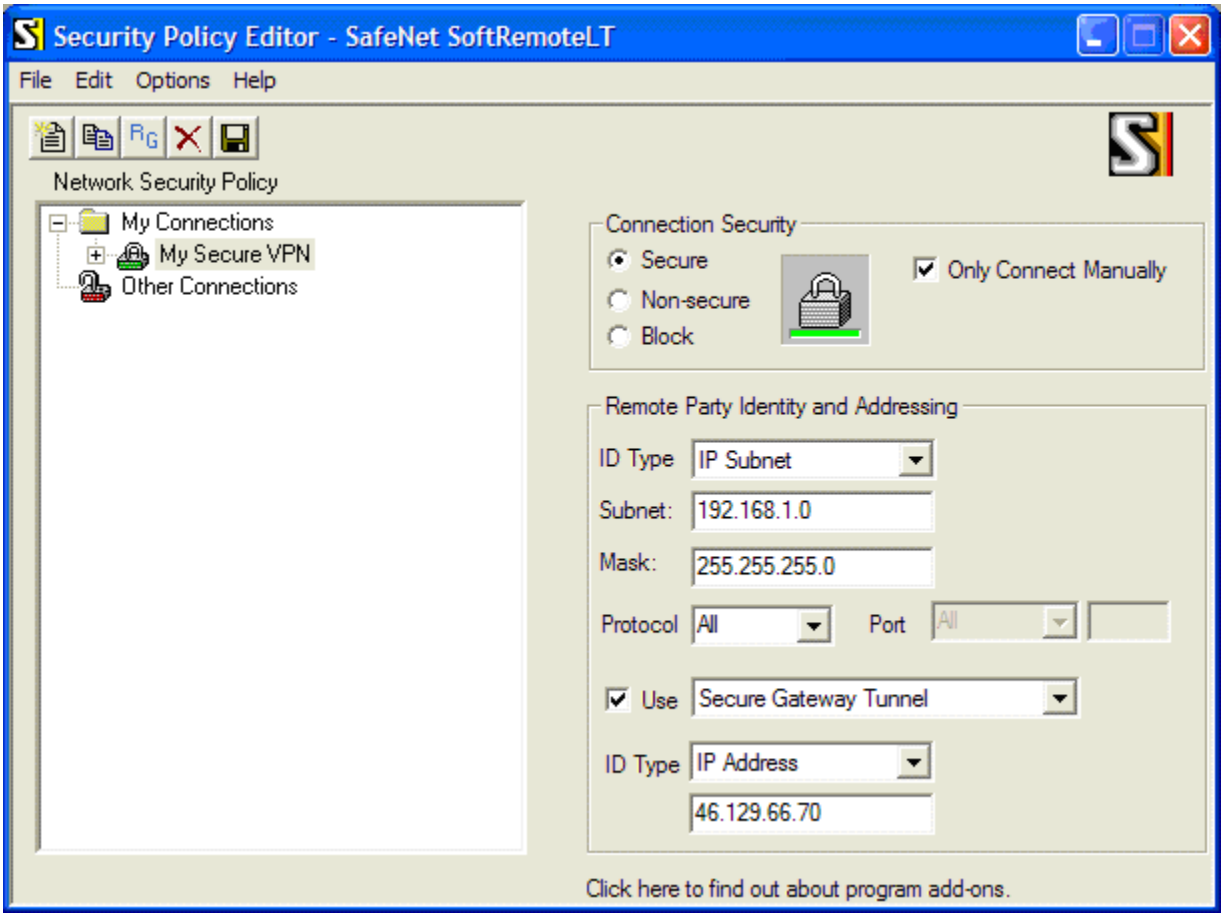
- Uninstall any IPSec VPN client that may be installed on your PC.
- Install SafeNet SoftRemote client by double clicking on the setup.exe file.
- Select the Typical installation option when prompted and client next begin the installation process.
- To finish the install process, restart your PC.
- Start the SoftRemote client by double clicking on the SafeRemote icon on your task bar
- From the menu bar, click on Edit ->Add->Connection



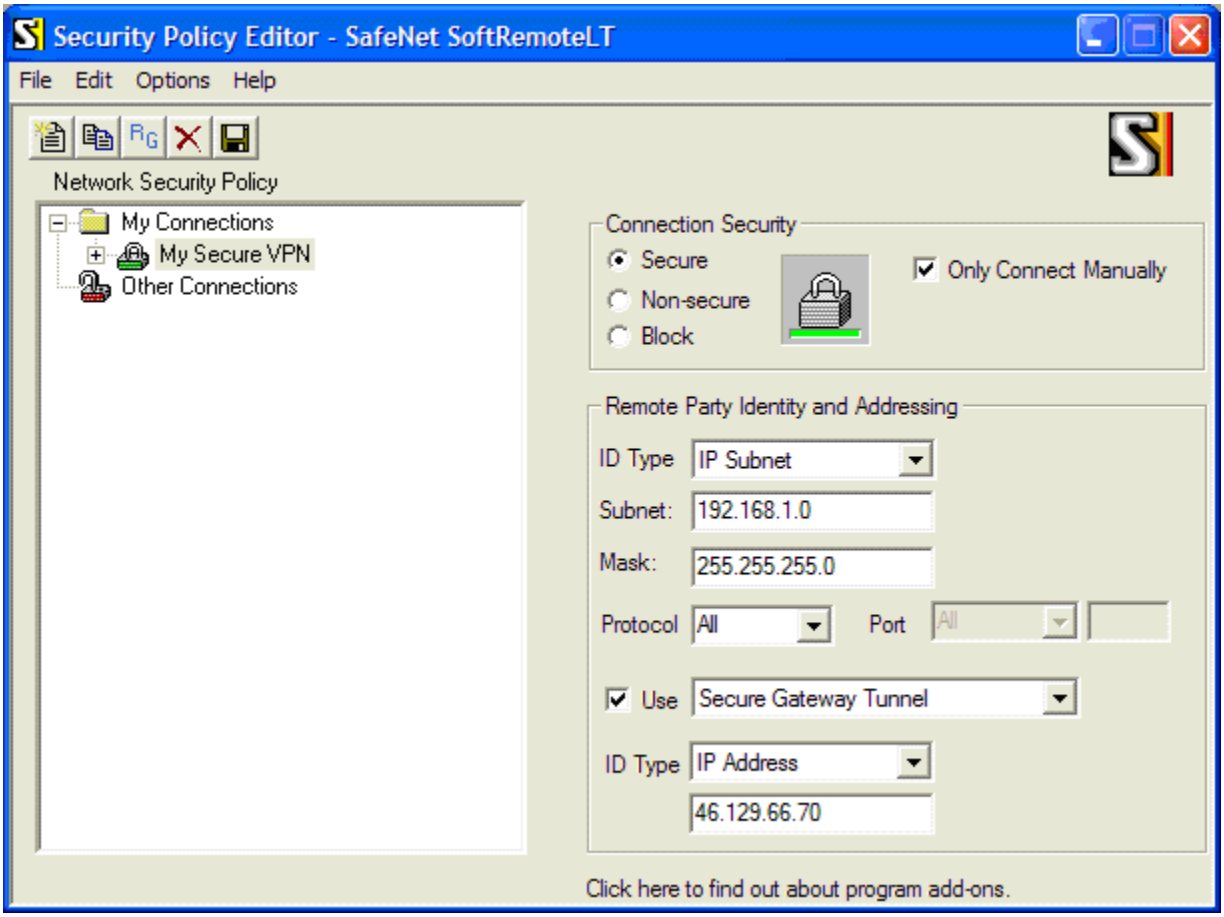
- Type in the name of your connection



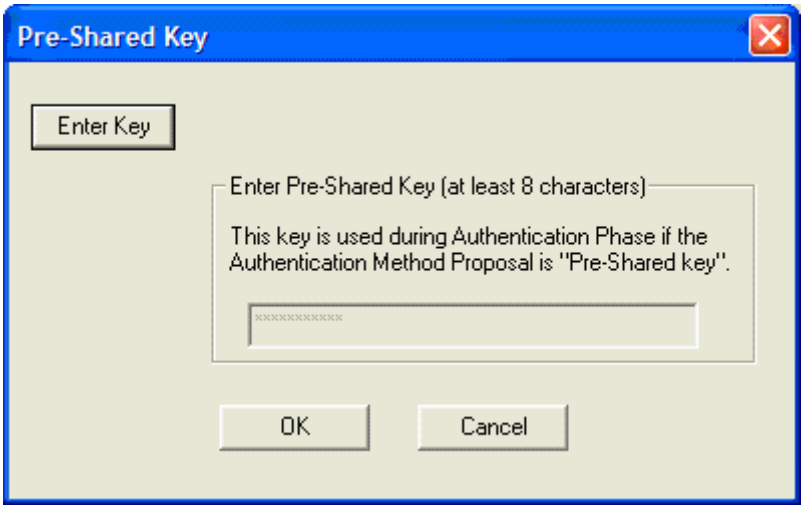
- Under Connection Security, make sure the Secure radio button is selected.
- Check the Only Connect Manually check box.
- In Remote Party Identity and Addressing, select the ID Type as IP Subnet.
- In the Subnet text box, specify the network address on the LAN side of BSG8ew to which the remote VPN client will be given access. In this example, we want the remote VPN users to have access to the employee Data VLAN. Hence set the Subnet address as 192.168.1.0. This value must match the policy configured.
- In the Mask text box, provide the subnet mask that corresponds the network address provide in Step ?12 above.
- In the Protocol drop-down list, select all.
- Select the Use checkbox and make sure Secure Gateway Tunnel is chosen from the drop-down list.



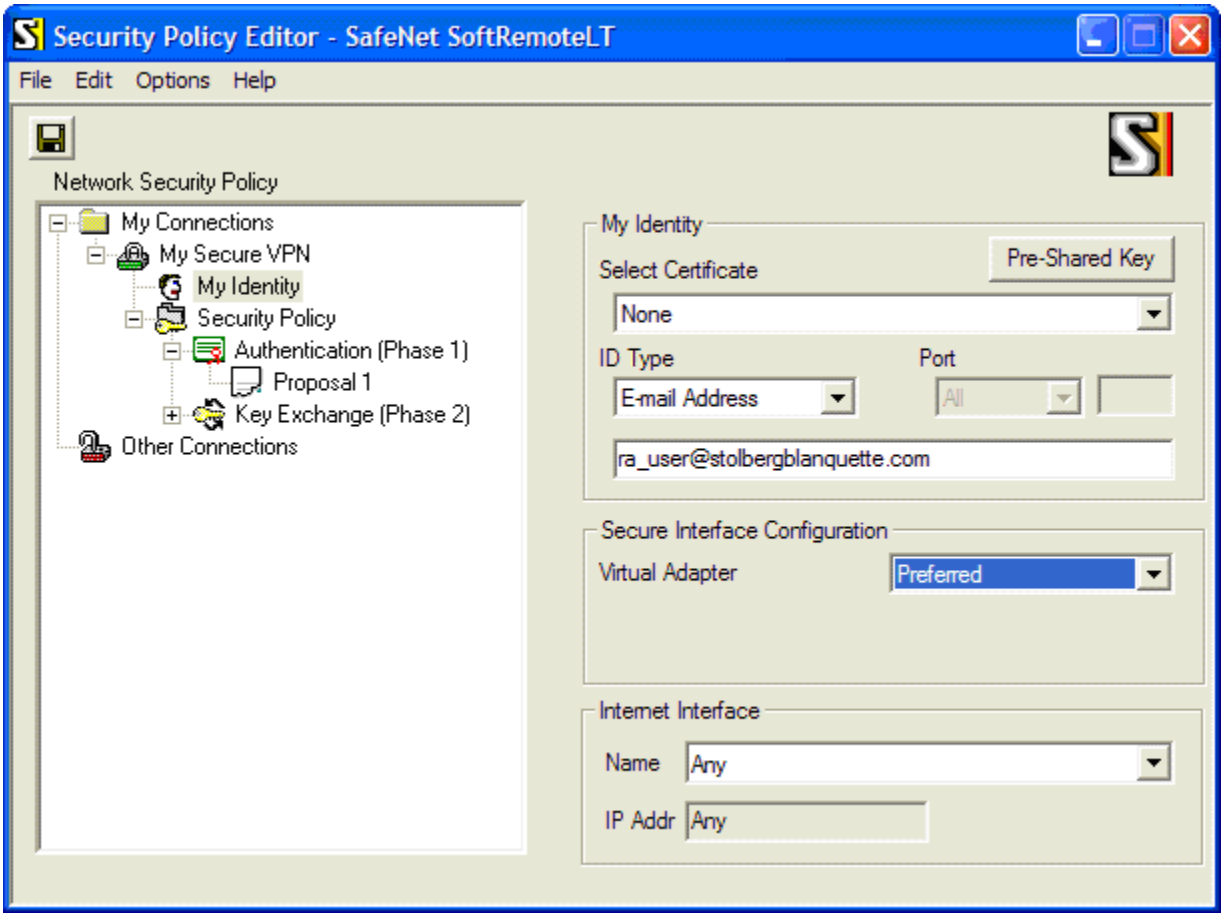
- In the **ID Type** for the remote gateway, select IP address and provide the IP address that was specified as the local identity of the BSG8ew. This is the IP address of the WAN interface of the BSG8ew.



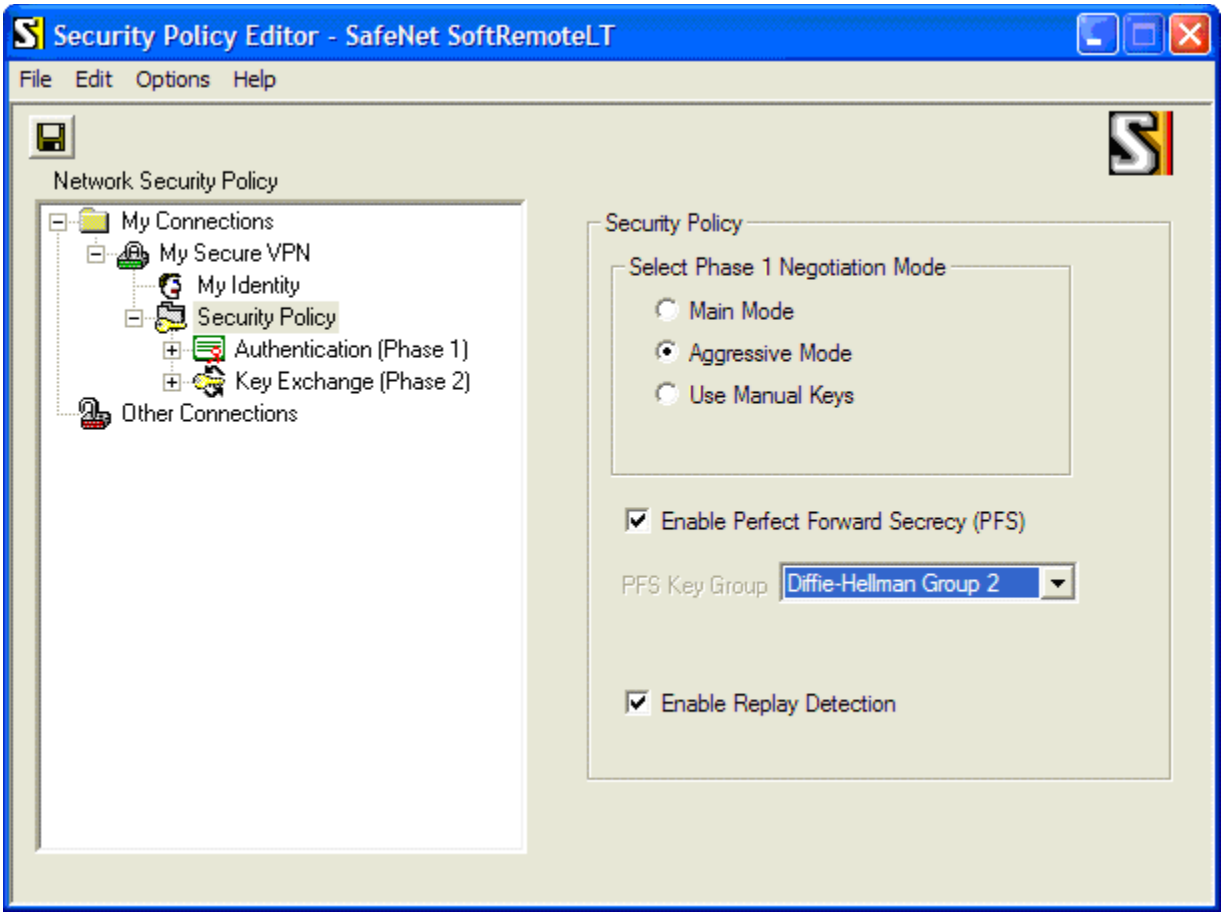
- Under **My Connections** in the in the Network Security Policy, expand the connection just created.
- Select My Identity.
- In the **Select Certificate** drop-down list, select none.
- Click the Pre-Shared Key button that appears.


Pre-Shared Key
Enter Key
Enter Pre-Shared Key (at least 8 characters)
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".
****
OK
Cancel

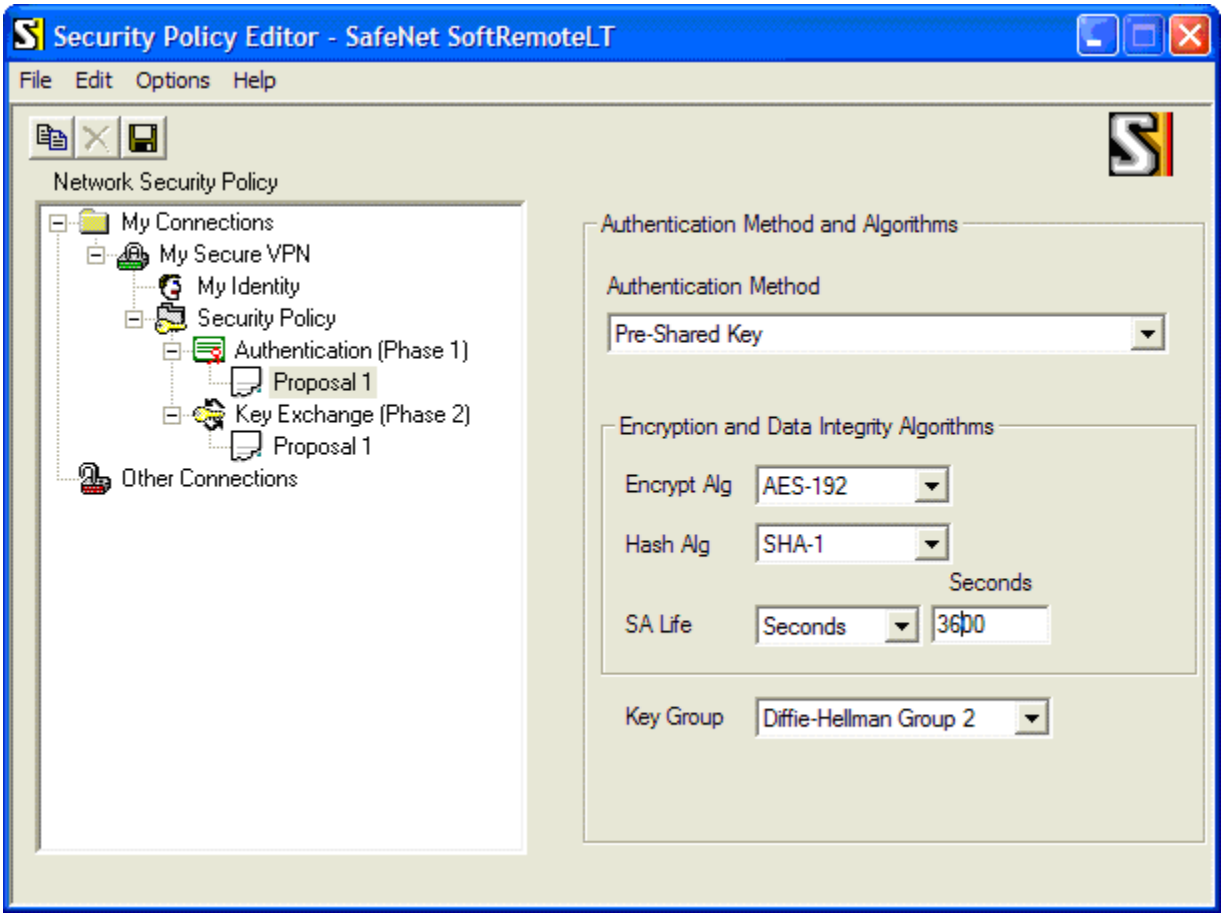
- Click on the **Enter Key** to provide the pre-shared key between the client and the BSG8ew and click OK. This value must match what was configured on the BSG8ew.
- Select the ID Type of the client as email and provide the email address that clients will be using. This must match what was configured on the BSG8ew.
- Under Secure Interface Configuration, set the Virtual Adapter as Preferred.



- Click on **Security Policy** under **My Identity** on the left.
- Select **Aggressive Mode** and check the checkbox next to **Enable Perfect Forward Secrecy (PFS)**.
- Select the Diffie-Hellman Group to use for PFS. This should match what is configured on the BSG8ew. For example, we have selected Diffie-Hellman Group 2 which matches what is configured on the BSG8ew.
- Enable **Replay Protection**



- Expand the Security Policy and click on Proposal 1 under Authentication (Phase 1).
- Choose **Encrypt Alg** as AES192 and **Hash Alg** as SHA-1. This must match what is configured on BSG8ew to protect IKE phase 1.
- Set the SA Lifetime in seconds and provide the value of the lifetime for phase 1 and the key Group Diffie-Hellman Group 2.



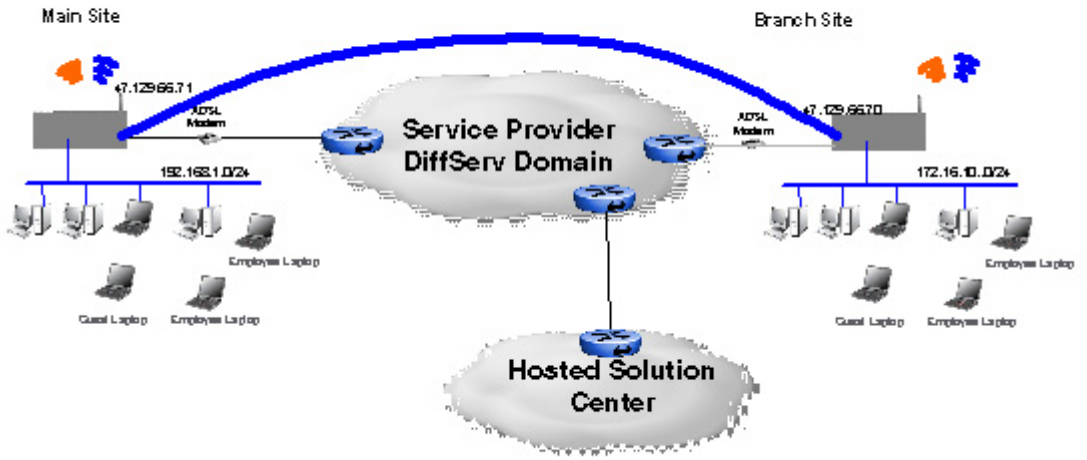
- Next click on **Proposal 1** under the Key Exchange (Phase 2).
- In IPSec Protocols section, provide the lifetime for IPSec Phase time. In this example we are using 3600 seconds.
- Make sure Compression is set to None.
- Under the Encryption and Data Integrity Algorithms,
  - — Select your Encrypt Alg. For example AES-192 for this example.
  - — Select your Hash Alg SHA-1 in this example.
  - — And set Encapsulation to Tunnel.
- Save your changes by clicking in File -> Save

Site to Site VPN topology

This section presents incremental provisioning procedure required to configure IPSec Branch Office tunnel between two customer sites.

Figure 36 – Customer topology with branch to branch IPSec tunnel presents the topology with tw

Figure 36 – Customer topology with branch to branch IPSec tunnel



Main site:

BSG8ew WAN Interface IP address: 47.129.66.71

Private network: 192.168.1.0/24

Branch site:

BSG8ew WAN Interface IP address: 47.129.66.70

Private network: 172.16.10.0/224

IPSec main site configuration

- Create a Site to Site VPN policy
- Configure BSG8ew at HQ to use a pre-shared to authenticate the remote end of the tunnel.
- Configure unit to use Tunnel mode
- Provide the identity of the remote end of the tunnel.
- Configure the HQ BSG8ew to use its WAN IP address as its identity.
- Provide the security association parameters for IKE
- Provide the IPSec security association parameters.

- Define an access list that defines the traffic that will be protected by this VPN policy.
- Configure the BSG8ew with the IKE pass phrase.
- Bind the configured policy to the WAN interface, in this case ppp 1.

Provisioning commands:

- `c t`
- `crypto map sitetosite`
- `crypto key mode preshared`
- `crypto map ipsec mode tunnel`
- `set peer 47.129.66.70`
- `isakmp local identity ipv4 47.129.66.71`
- `isakmp policy encryption aes-192 hash sha1 dh group2 exch main lifetime se 3600`
- `crypto map ipsec encryption esp aes-192 authentication esp sha1 pfs group2 lifetime secs 3600`
- `access-list apply any source 192.168.1.0 255.255.255.0 destination 172.16.10.0 255.255.255.0`
- `exit`
- `vpn remote identity ipv4 47.129.66.70 psk 1qazxsw2`
- `interface ppp 1`
- `crypto map sitetosite`
- `end`
- `write startup-config`

IPSec branch site configuration

- Create a Site to Site VPN policy
- Configure BSG8ew at the remote office to use a pre-shared to authenticate the remote end of the tunnel.
- Configure unit to use Tunnel mode
- Provide the identity of the remote end of the tunnel.
- Configure the remote office BSG8ew to use its WAN IP address as its identity.
- Provide the security association parameters for IKE
- Provide the IPSec security association parameters.
- Define an access list that defines the traffic that will be protected by this VPN policy.
- Configure the BSG8ew with the IKE pass phrase.
- Bind the configured policy to the WAN interface, in this case ppp 1.

Provisioning commands:

- `c t`
- `crypto map sitetosite`
- `crypto key mode preshared`
- `crypto map ipsec mode tunnel`
- `set peer 47.129.66.71`
- `isakmp local identity ipv4 47.129.66.70`
- `isakmp policy encryption aes-192 hash sha1 dh group2 exch aggressive lifetime se 3600`
- `crypto map ipsec encryption esp aes-192 authentication esp sha1 pfs group2 lifetime secs 3600`
- `access-list apply any source 172.16.10.0 255.255.255.0 destination 192.168.1.0 255.255.255.0`
- `exit`
- `vpn remote identity ipv4 47.129.66.71 psk 1qazxsw2`
- `interface ppp 1`
- `crypto map sitetosite`
- `end`

Appendix A – SMB solution integration with BCM50

This section introduces BCM50 to the SMB architecture presented in this document. The information provided in this section is valid for BCM50 Release 1, 2 and 3. The detailed description of the various configuration options is provided in sections below. There are four configurations that are considered with BCM50 located on the customer site.

- One site configuration with Unistim IP Phones only (Figure 37 – Single site - UNISTIM phones only (page 164))
- One site configuration with Unistim IP Phones and with LG 6800 SIP Phones (Figure 38 – Single site - UNISTIM and LG6800 phones (page 166))
- Site-to-site configuration with one BCM50 site (Figure 39 – Site-to-Site with one site BCM50 (page 167))
- Site-to-site configuration with two BCM50 sites (Figure 40 – Site-to-Site with SIP trunks (page 168))

From BCM50 perspective, associated UNISTIM phones BSG8ew has a role of a router and it provides data services specifically:

- IP routing and forwarding
- IP Sec branch and client tunnels
- DHCP Server – to assign IP address to the BCM50
- QoS

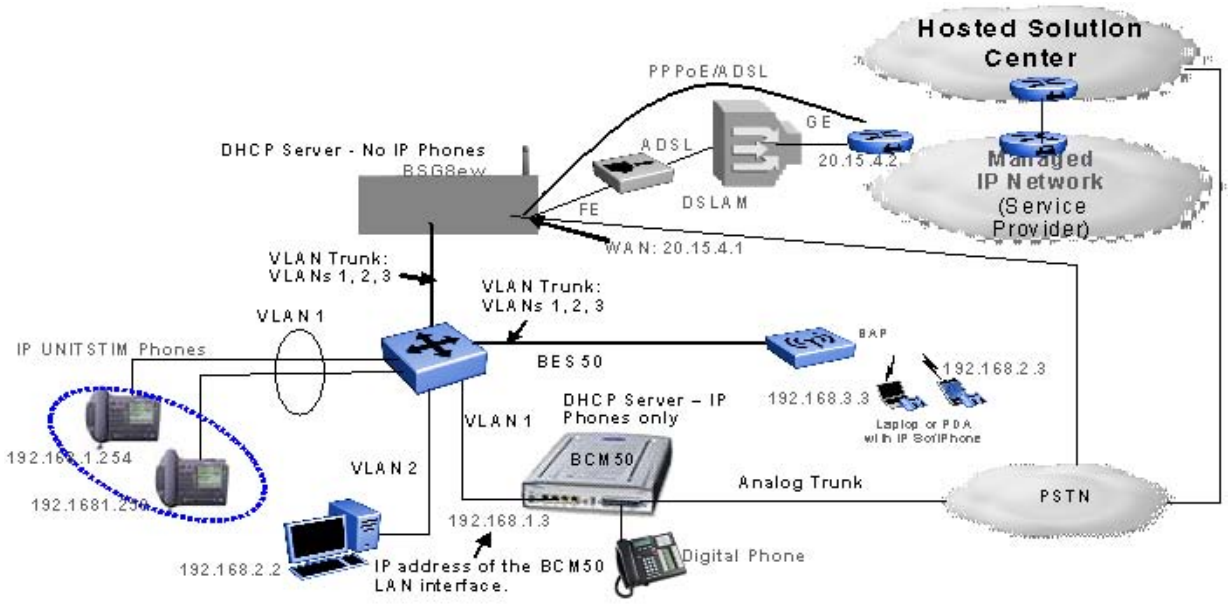
The UNISTIM phones communicate with the UTPS Server on the BCM50 for call control. The LG SIP sets as in other topologies use SIP Proxy and Registrar services on the BSG8ew.

Single site — UNISTIM phones only

In the configuration presented in Figure 35 - Customer network topology (page 96) the BCM50 provides telephony services to digital and UNISTIM IP Phones. The BSG8ew provides for the data services to the customer devices including management access to the BCM50.

To allow external calls BCM50 is connected to the PSTN network by means of analog trunks. Details of configuring BCM50 analog trunks is outside of the scope of this document and can be found in documentation for the BCM50 product.

Figure 37 – Single site - UNISTIM phones only



Current default settings for BSG8ew and BCM50 provide for automatic configuration and enabling of telephony services for UNISTIM phones.

The DHCP Server BSG8ew assigns IP addresses to all the devices on the customer LAN with exception to the UNISTIM IP phones. The UNISTIM IP phones are assigned IP addresses by the BCM50 DHCP Server. The BCM50 DHCP server is by default enabled only for UNISTIM phones (by means of DHCP Vendor ID and Nortel proprietary DHCP options).

The BCM50 DHCP Server pool range is by default 192.168.1.200 – 192.168.1.254, so it does not overlap with the default BSG8ew DHCP Server range of 192.168.1.1 – 192.168.1.127.

The BCM50 has by default DHCP client enabled on its LAN interface. When BCM50 boots up, its DHCP client starts DHCP protocol to acquire IP address from available DHCP server. The BSG8ew DHCP server needs to be available at the time when BCM50 boots up otherwise BCM50 will assign 192.168.1.2 address to its LAN interface. BCM50 automatically updates default gateway attribute for its DHCP server to be BCM50 LAN interface address. The primary and secondary terminal proxy servers, S1 and S2 are set to be IBCM50 LAN interface IP address. The S1 and S2 are distributed to the UNISTIM IP sets in DHCP OFFER message.

The BCM50 as well as UNISTIM phones are members of the voice VLAN 1, 192.168.1.0/24. Additional VLANs, for example data and guest VLAN is added as for other topologies.

The BSG8ew DHCP server should be configured assign a reserved IP address to the BCM50 LAN interface (based on its MAC address). This will help to identify BCM50 when accessing it for management purposes. For example, BSG8ew DHCP server is configured to assign 192.168.1.3 to BCM50 LAN interface.

BCM50 can be part of any VLAN, however both BCM50 and the UNISTIM phones have to be members of the same VLAN.

Below is the example of attributes that the BCM50 will provide in DHCP OFFER message to UNISTIM IP phones in addition to the phone IP address:

- S1 IP address: 192.168.1.3
- S1 Port: 7000
- S1 Action: 1
- S1 Retry Times: 1
- S2 IP address: 192.168.1.3
- S2 Port: 7000
- S2 Action: 1
- S2 Retry Times: 1

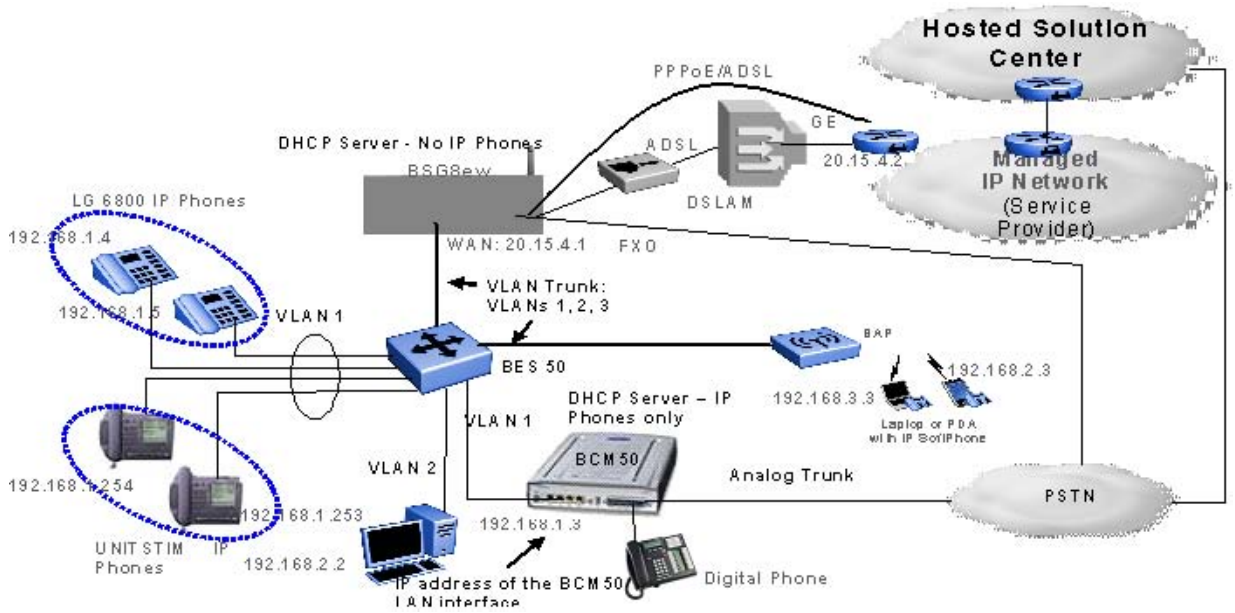
Single site — UNISTIM and LG phones

A BCM50 role in this configuration is no different from configuration in Single site — UNISTIM phones only (page 163) section. In this configuration, however BSG8ew is configured as a SIP proxy and SIP registrar to provide SIP line services to the LG 6800 SIP phones. The SIP line services are provided as previously described in this document. Both LG and UNISTIM phones as well as BCM50 are members of the same voice VLAN and VLAN1.

LG phones register with the Host Solution Center (HSC) SIP server through BSG8ew SIP proxy. UNISTIM phones register with the BCM50 UTPS server.

The UNISTIM end points are assigned with IP addresses by the BCM50 DHCP server from the range of 192.168.1.200- 192.168.1.254. The LG phones are assigned their IP addresses by the BSG8ew DHCP server from the range of 192.168.1.1 – 192.168.1.127. Thus, there is no overlapping of addresses between the two DHCP servers.

Figure 38 – Single site - UNISTIM and LG6800 phones



From BCM50 perspective the calls from LG phones are external calls and they have to cross PSTN network for both signaling and media to terminated on UNISTIM phones.

Site-to-Site configuration

In a site-to-site configuration the two sites are connected with the IPSec Branch Office tunnel. There are two options here:

- BCM50 present only at Main site. All the phones from both Main and Branch sites need to register with that one BCM50 (Figure 39 – Site-to-Site with one site BCM50 (page 167)).
- BCM50 present at Main and Branch sites. The calls between the sites are made by means of SIP or H.323 trunks between the two BCM50s (Figure 40 – Site-to-Site with SIP trunks (page 168)).

In both cases configurations can be expanded by the addition of LG phones and use of BSG8ew SIP server along with Hosted Solution Services described in this document.

At the main site the IP addresses are assigned by BSG8ew DHCP server as well as BCM50 DHCP server. BCM50 DHCP server assigns IP addresses to UNISTIM sets only. The BSG8ew DHCP server serves all other devices including LG phones.

For the configuration presented in Figure 39 – Site-to-Site with one site BCM50 (page 167), the UNISTIM sets at the branch site can not be served by the BCM50 located at the main site. Thus they need to be provisioned manually or use the BSG8ew DHCP server for IP address assignment in partial configuration mode. The IP address of the UTPS server (S1/S2), which is the IP address of the BCM50 LAN interface hast to be assigned manually for branch site UNISTIM sets.

The calls originated from UNISTIM phones and destined outside of site 1 and site 2 are completed by means of analog trunks to PSTN.

Figure 39 – Site-to-Site with one site BCM50

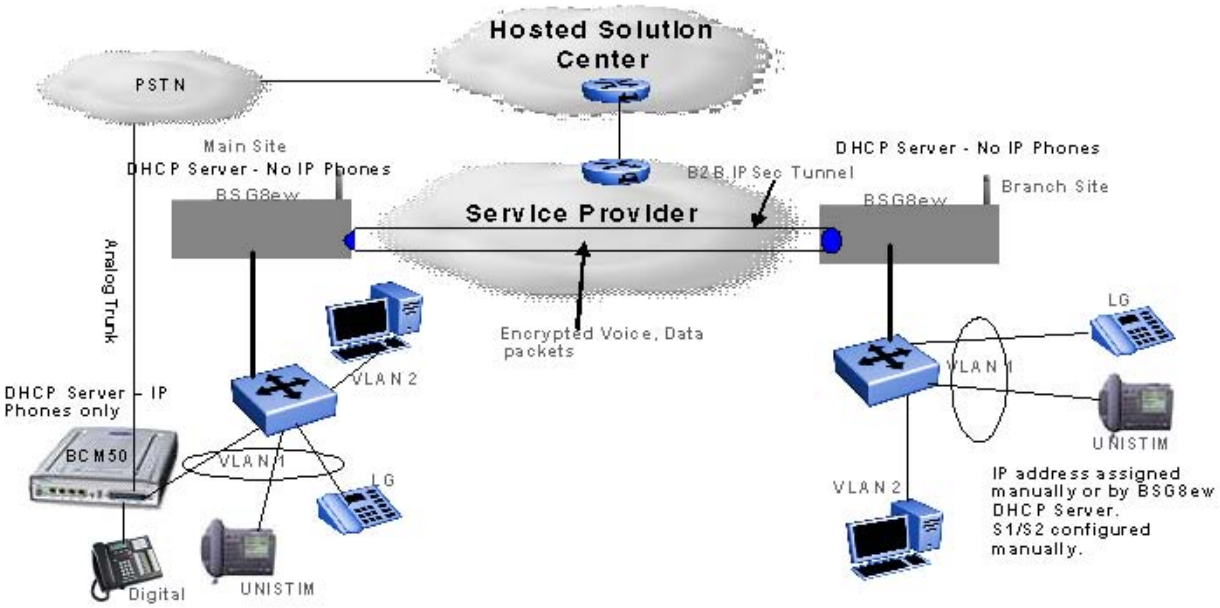
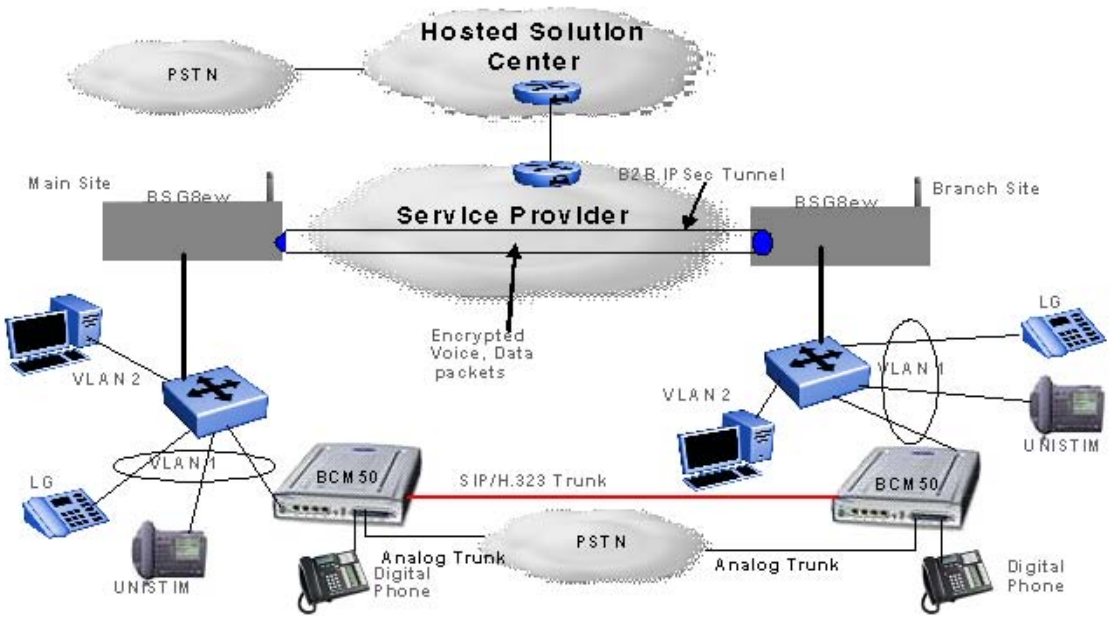


Figure 40 – Site-to-Site with SIP trunks (page 168) shows the case when there is a BCM50 present at both main and branch sites. In this case, the UNISTIM phones register with the local BCM50. IP addresses are assigned as previously described. The DHCP server on BCM50 serves UNSITIM sets and the DHCP server on BSG8ew serves all the customer devices except of UNISTIM phones. The VoIP calls between UNISTIM sets at two sites are made by means of SIP or H.323 trunks that are established between the two BCM50s.

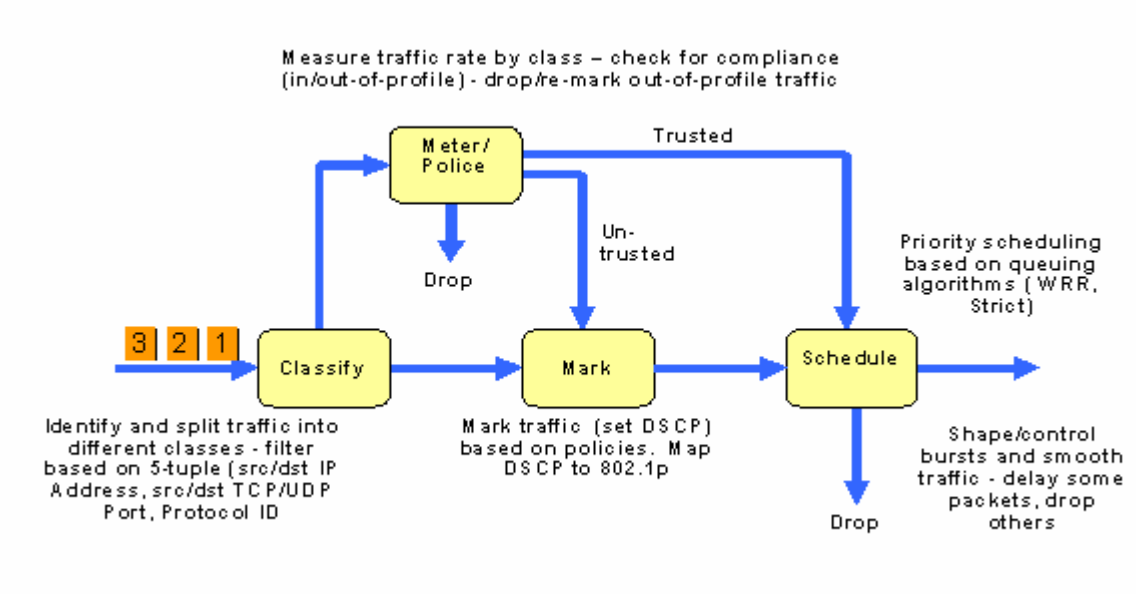
Figure 40 – Site-to-Site with SIP trunks



Appendix B – QoS architecture of BSG8ew

The QoS architecture available in the solution is build with a standard QoS components presented in Figure 34 – Reference topology 4 (page 92). The BSG8 model supports all the components with the exception of shaping. Figure 37 – Single site - UNISTIM phones only (page 164) shows the path that packet takes through QoS system.

Figure 41 End-to-end diffServ domain


Measure traffic rate by class – check for compliance (in/out-of-profile) - drop/re-mark out-of-profile traffic
Meter/ Police
Trusted
Un-trusted
Drop
Priority scheduling based on queuing algorithms (WRR, Strict)
3
2
1
Classify
Mark
Schedule
Identify and split traffic into different classes - filter based on 5-tuple (src/dst IP Address, src/dst TCP/UDP Port, Protocol ID
Mark traffic (set DSCP) based on policies. Map DSCP to 802.1p
Drop
Shape/control bursts and smooth traffic - delay some packets, drop others

Classification

In the solution the BSG8ew is responsible for classification of the packets received from the customer devices prioritizing them based on the classification and if necessary marking them with proper DSCP to match the DiffServ domain they are entering.

The classification of the packets is done on both WAN and LAN interfaces. The packets are classified on the following:

- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- DSCP or
- 802.1p priority bits

Congestion control

In addition to packet prioritization it is important that the available bandwidth is managed in order to prevent the packet loss but at the same time avoid starvation of less important traffic.

To avoid excessive loss of packets the congestion in the egress queues has to be controlled. The BSG8ew supports tail drop, random early detection and weighted random early detection algorithms for congestion avoidance.

Meter / Policer

The traffic meter measures the temporal properties of packets selected by the classifier against a configured traffic profile. The meter passes the state information to the Policer to trigger a particular policing action for each packet that is either in-profile or out-of-profile.

The BSG8ew supports the Two Rates, Three Color Meter (TRTCM) policing algorithm.

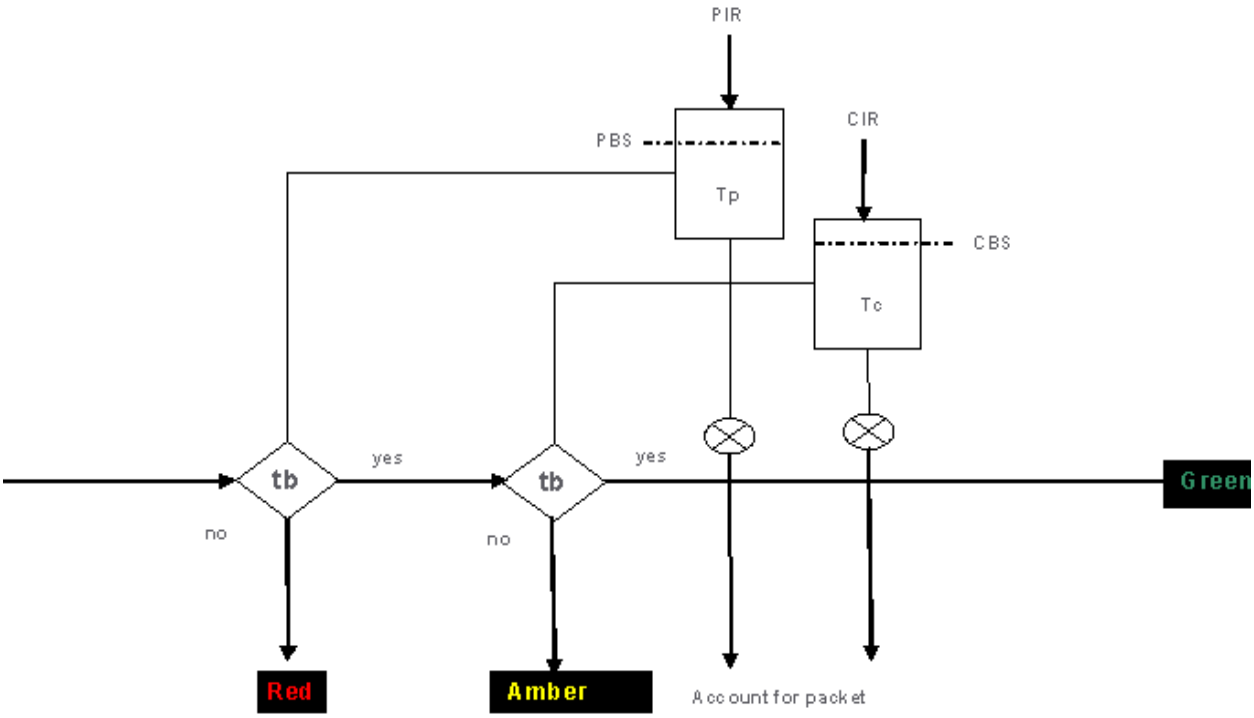
The algorithm allows one to specify the Peak Information Rate (PIR), Committed Information Rate (CIR), their corresponding burst sizes, i.e., Peak Burst Size (PBS) and Committed Burst Size (CBS) respectively for a flow.

The implementation makes use of two token buckets: Token bucket C and Token bucket P. Token Bucket C is used to monitor the CIR and Token Bucket P is used to monitor the PIR. The depth of Token Bucket C is equal to Committed Burst Size (CBS) and its token count, T_c, is updated at the CIR rate. The depth of Token Bucket P is Peak Burst Size (PBS) and its token count T_p is initially set to PBS and is updated at PIR rate.

Figure 42 – TRTCM Policer (page 171) shows the TRTCM operation in BSG8ew. An ingress packet of size B bytes arriving at time *t* is first compared with the token count of Bucket P, T_p. If Bucket P does not have enough credit, i.e, $B > T_p$, the packet is marked red regardless of Bucket C, and no changes are made to T_c and T_p.

If Bucket P has enough credit, i.e., T_p B, the packet size is compared with token count of Bucket C, T_c. If $T_c < B$, the packet is marked amber. If on the other hand T_c B, bucket P has enough credit, i.e., T_p B, the packet is marked green.

Figure 42 – TRTCM Policer

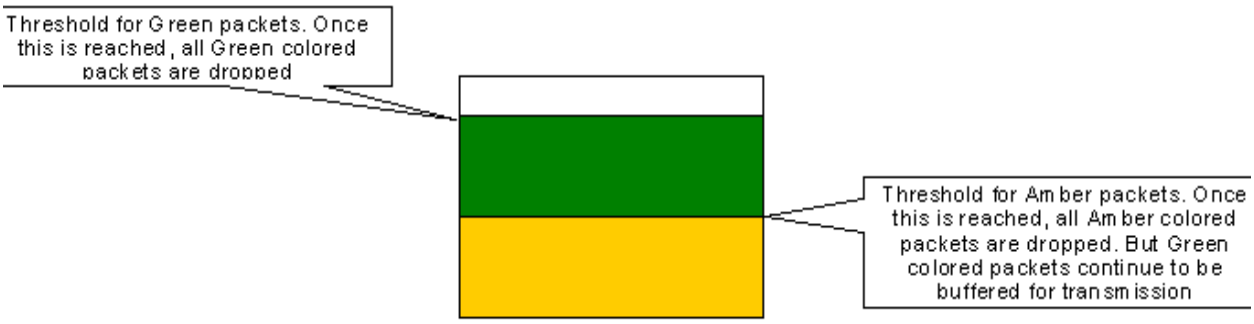


The output of the policer is then used by the congestion avoidance algorithm to decide whether to enqueue the packet for transmission or discard the packet. Red colored packets are dropped right away regardless of what congestion avoidance algorithm is in use. Depending on the state of the egress queue and the configured congestion avoidance algorithm, green and amber colored packets are enqueued for transmission or discarded.

Congestion avoidance

The BSG8ew supports three congestion avoidance algorithms: Tail Drop, Random Early Detection (RED) and Weighted RED. In the BSG8ew, the Tail Drop algorithm is used for non-TCP flows and enqueues both amber and green packets as long as the queue up to their respective configured thresholds. Once the threshold for a particular color is reached, the algorithm starts to drop those packets while enqueuing the other colored packets provided its threshold is greater.

Figure 43 Tail-Drop congestion avoidance

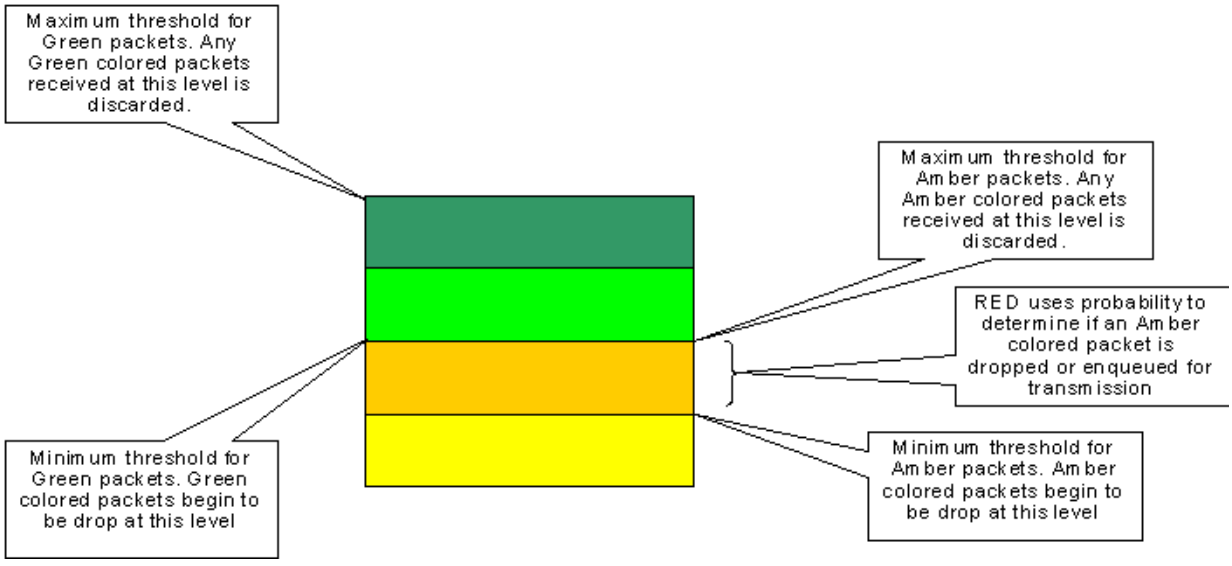

Threshold for Green packets. Once this is reached, all Green colored packets are dropped
Threshold for Amber packets. Once this is reached, all Amber colored packets are dropped. But Green colored packets continue to be buffered for transmission

RED by contrast works on only TCP based flows in the BSG8ew and starts dropping packets before the egress queue overflows. In BSG8ew, the RED algorithm achieves this by monitoring the average queue sizes and drops packets based on statistical probabilities from flows before a hard limit is reached. This causes a congested link to slow more gracefully and prevents retransmit synchronization. Minimum and maximum thresholds are configured for both Green and Amber colored packets.

The algorithm begins to drop packets when the average queue depth is above the configured minimum threshold for that colored packets. The rate of drop of packets of that color increases linearly until the maximum threshold configured for packets is reached at which point, all arriving packets of that color are dropped.

Weighted Random Early Detect (WRED) uses the capabilities of RED but in addition can provide further QoS differentiation between the different colors if the configured thresholds for Green are greater than those for Amber packets.

Figure 44 WRED congestion avoidance


Maximum threshold for Green packets. Any Green colored packets received at this level is discarded.
Maximum threshold for Amber packets. Any Amber colored packets received at this level is discarded.
RED uses probability to determine if an Amber colored packet is dropped or enqueued for transmission
Minimum threshold for Green packets. Green colored packets begin to be drop at this level
Minimum threshold for Amber packets. Amber colored packets begin to be drop at this level

Once enqueued, all packets are treated equally regardless of color and it is now the role of the scheduler to decide when a particular packet will be transmitted.

Scheduler

Two scheduling algorithms are supported by the BSG8ew: Deficit Weighted Round Robin (DWRR*)* and Strict priority. Each of the eight CoS queues can be configured to use on or the other algorithm by the value assigned to that CoS queue. Weights of value zero configures a CoS queue to be scheduled using Strict Priority. Any other weight assigned to a queue configures that queue to use DWRR.

Strict Priority scheduling is specially designed for delay/jitter-sensitive traffic such as voice. Queues configured to use strict priority are serviced in preference to other queues. They are always serviced regardless of the states of the other queues configured to be scheduling using DWRR.

The DWRR scheduler services the queues in the ratio of the configured weights. Higher weights translate to proportionally higher bandwidth and lower latency.

One or more of eight CoS queues can be configured for Strict Priority. When configuring more than one queue for strict priority, the configured queues must be adjacent to each other. For example one cannot configure CoS 0 and 2 for strict priority and configure CoS queue 1 for DWRR.

Call admission control

The Call Admission Control (CAC) function ensures there is adequate WAN bandwidth for both incoming and outgoing call before the call is setup. CAC tracks the number of current calls established across the WAN link and does not allow this number to exceed a configured value.

Appendix C - BSG8ew services

This section describes the different types of features used in BSG8ew.

Feature	Standard
Layer2 Switching	
Port based VLANs (independent VLAN learning)	802.1Q - 1998
Protocol based VLANs	802.1v
GVRP support	802.1D
Tunneling (VLAN stacking or Q-in-Q)	802.1Q
Rapid Spanning Tree Protocol	802.1D, 2004
Multiple Spanning Tree	802.1s
Port Based Authentication with EAP	802.1X-REV2004
PPPoE	
IPv4 routing	
Static routing	RFC 1812
RIP v1/v2	RFC 2453, 2091, 2082
OSPFv2	RFC 1765, 1793 2328, 2370
Inter VLAN routing	
Route Redistribution	
Redundancy	
VRRP	RFC 2338
Telnet server	RFC 854, 855, 856, 858
TFTP client	RFC 1350
Ethernet ARP	RFC 826
IGMP router (v1, v2 and v3)	RFC 3376
Message Digest Algorithm	RFC 1321
Radius client	RFC 2138
TACACS+ client	Draft-ietf-grant-02
DHCP client, server, relay agent	RFC 2131, 2132
QoS	
Priority based switching	802.1p
DiffServ	
Management and administration	
SNMP v1	RFC 1155, 1157, 1212, 1213, 1215, 2089, 2578, 3411, 3412, 3413, 3414, 3415, 3416, 3417 (partial), 3584

SNMP v2c	
SNMP v3	
CLI (telnet and console)	NA
WebUI (embedded HTTP server)	RFC 1945
Multiple Levels of user privileges (CLI and WebUI)	NA
SSL Protocol Version 3.0	RFC 2246
TLS (Transport Layer Security) Version 1.0	RFC 2246
SSH Protocol Version 2.0	draft-ietf-secsh-architecture-12.txt, draft-ietf-secsh-transport-14.txt, draft-ietf-secsh-userauth-15.txt, draft-ietf-secsh-connect-15.txt
Power Over Ethernet management	IEEE 802.1af
MIB support	
MIB II	RFC 1213
MIB II for SNMPv2	RFC 3418
SNMP Community MIB	RFC 3584
SNMP Message Processing and Dispatching MIB	RFC 3412
SNMP Notification MIB	RFC 3413
SNMP Target MIB	RFC 3413
SNMP User Based Security Model MIB	RFC 3414
SNMP View Based Access Control MIB	RFC 3415
Interface group MIB	RFC 2233
VLAN MIB	RFC 2674
Spanning Tree Protocol MIB	RFC 1493
Rapid STP MIB	draft-ietf-bridge-rstpmib-02;
Multiple STP MIB	Proprietary MIB
Port-based Network Authentication Control MIB	IEEE 802.1 X
Radius Client MIB	RFC 2618
IPv4 MIB	RFC 2011, 2013, 2096; Additional Proprietary MIB
IGMP MIB	draft-ietf-magma-rfc2933-update-00.txt
DHCP	Proprietary MIB
RIP v1/v2 MIB	RFC 1723; 1724, 2453 Additional Proprietary MIB
OSPFv2 MIB	RFC 1850; Additional Proprietary MIB
VRRP MIB	RFC 2787

Security	
ACL (Access Control List)	NA
State full Inspection Firewall	NA
NAT	RFC 1631
WPA2 wireless security	802.11i 2004
VPN	
IPSec - Security Architecture for IP	RFC 2401
IP Authentication Header (AH)	RFC 2402
Use of HMAC-MD5-96 with AH and ESP	RFC 2403
Use of HMAC-SHA1-96 with AH and ESP	RFC 2404
ESP AES, 3-DES, DES-CBC Cipher Algorithm with Explicit IV	RFC 2451
IP Encapsulation Security Payload (ESP)	RFC 2406
NULL Encryption Algorithm and its use with IPSec	RFC 2410
MD5 Message-Digest Algorithm	RFC 1321
IP Authentication using keyed MD5	RFC 1828
IKE - The IP Security Domain of Interpretation for ISAKMP	RFC 2407
Internet Security and Key Management Protocol	RFC 2408
Internet Key Exchange	RFC 2409
The Oakley Key Determination Protocol	RFC 2412
WiFi LAN access	
WiFi interface	802.11 b/g
Extensible authentication protocol	RFC 3748
SIP	
SIP service support	RFC 3261, RFC 3262, RFC 2976, RFC 3311, RFC 3326
Bearer DTMF support (RFC 2833 to SIP user info)	